Office of Inspector General | United States Postal Service

Audit Report

Informed Visibility Vulnerability Assessment

Report Number IT-AR-19-001 | October 12, 2018

Table of Contents

Highlights

Objective

Our objective was to evaluate the Informed Visibility (IV) system's externally-facing and supporting servers and databases to determine whether they comply with U.S. Postal Service security control requirements and industry best practices; and whether they pose a risk to the confidentiality, integrity, and availability of the system. The security-related information in this report reflects a specific point in time and may have changed since our testing.

The IV system provides full mail visibility for all mail and packages through the entire mail stream. The Postal Service is leveraging this system to compete in today's marketplace to gain customers' confidence that mail is a relevant communication medium. IV is intended to improve the customers' ability to make better business decisions by providing them with greater access to near real-time tracking data. The Postal Service began deployment activities for IV in November 2014, and incorporated the [redacted] database management system into IV starting in February 2017. The Postal Service completed implementation of the IV system in September 2017.

> *"The IV system provides full mail visibility for all mail and packages through the entire mailstream."*

What the OIG Found

Overall, the Postal Service complied with Postal Service security control requirements and industry best practices for the externally-facing and supporting IV servers and databases. However, we identified four opportunities to strengthen the system's security posture and reduce the risk to the confidentiality, integrity, and availability of the system.

First, the 13 IV servers we reviewed were generally in compliance with the Postal Service configuration baseline, which defines the system settings for these servers. However, we identified some system misconfigurations on each of these servers. These misconfigurations occurred because system administrators [redacted] In addition, while comparing the configuration baseline to industry benchmarks, we identified recommended security settings that the Postal Service did not include in its baseline document.

Second, while the overall IV web application encryption and authentication were secure, we identified three encryption and authentication vulnerabilities related to communication protocols. This occurred because these protocols were not identified for upgrade during the Postal Service's IV web application configuration review. These vulnerabilities would allow an attacker to [redacted] Management took corrective action to remediate all three vulnerabilities by upgrading to the latest version of the communication protocol.

Third, while the [redacted] databases we reviewed provided limited account management functionality, we identified weaknesses in account management controls, specifically with password complexity, disabling user accounts, and maintaining audit logs. This occurred because these databases currently do not have the capability to fully implement Postal Service user account management and logging requirements.

Without account management controls, the IV system is at risk for [redacted]. Further, if expired accounts are not disabled in a timely manner, this increases the duration that Postal Service information resources are vulnerable to compromise. Additionally, without audit logs, the Postal Service would not be able to obtain sufficient detail to reconstruct activities in the event of a compromise or malfunction.

Lastly, the Postal Service has not fully developed a configuration baseline for the IV [redacted] databases. Since the Postal Service had not used [redacted] databases before, management was not aware they needed to create a configuration baseline. [redacted]

[redacted] In 2018, management began drafting a [redacted].

What the OIG Recommended

We recommended management:

- Develop a process to ensure that IV server configurations comply with the established configuration baseline.
- Review the controls identified in the industry benchmarks and consider including them in the published standard.
- Include communication protocols in future IV web application configuration reviews and address any identified control weaknesses.
- Implement account management controls for the databases to meet Postal Service requirements.
- Enable the audit logging function for the databases or approve a risk acceptance letter.
- Finalize, publish, and implement the [redacted] configuration baseline document.

Transmittal Letter

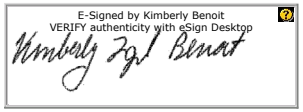
OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

October 12, 2018

MEMORANDUM FOR: ISAAC S. CRONKHITE
VICE PRESIDENT, ENTERPRISE ANALYTICS

GREGORY S. CRABB
VICE PRESIDENT, CHIEF INFORMATION SECURITY OFFICE

JEFFREY C. JOHNSON
VICE PRESIDENT, INFORMATION TECHNOLOGY



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

SUBJECT: Audit Report – Informed Visibility Vulnerability Assessment (Report Number IT-AR-19-001)

This report presents the results of our audit of the Informed Visibility Vulnerability Assessment (Project Number 18TG001IT000).

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: Postmaster General
Corporate Audit Response Management

Results

Introduction/Objective

This report presents the results of our self-initiated vulnerability assessment of the U.S. Postal Service's Informed Visibility (IV) system (Project Number 18TG001IT000). Our objective was to evaluate the IV system's externally-facing[1] and supporting servers and databases to determine whether they comply with Postal Service security control requirements and industry best practices; and whether they pose a risk to the confidentiality, integrity, and availability of the system. The security-related information in this report reflects a specific point in time and may have changed since our testing. See Appendix A for additional information about this audit.

Background

The IV system provides full mail visibility for all mail and packages through the entire mail stream (i.e., induction, transport, and delivery). The Postal Service is leveraging this system to compete in today's marketplace to gain customers' confidence that mail is a relevant communication medium. IV is intended to improve the customers' ability to make better business decisions by providing them with greater access to near real-time tracking data.

In 2014, the Postal Service adopted a strategy to achieve full visibility of mail as it moves through the mailstream. This strategy included providing users with access to business and operational intelligence resulting in better informed decisions for operations, sales, finance, marketing, and revenue functions. To achieve this initiative, the Postal Service began deployment activities of the IV system in November 2014 and incorporated the [redacted] database management system into IV starting in February 2017. The Postal Service completed implementation of the IV system in September 2017 for use by internal and external customers. To increase IV system performance, the Postal Service deployed an additional 1,300 servers in July 2018.

Overall, the Postal Service complied with Postal Service security control requirements and industry best practices for the externally-facing and supporting IV servers and databases. However, we identified opportunities to strengthen the

1 Externally-facing and supporting servers and databases support the customer's business operations, for example business mailers who use the Postal Service's IV Mail Tracking and Reporting capabilities.

systems security posture to reduce the risk to the confidentiality, integrity, and availability of the system.

Finding #1: Configuration Baseline Compliance

The 13 IV servers we reviewed were generally in compliance with the Postal Service configuration baseline,[2] which defines the system settings for these servers. However, we identified some system misconfigurations on each of these servers[3] [redacted] We found that all 13 servers contained between three and eight configurations that did not comply with Postal Service policy.

Postal Service policy[7] states that information resources hosting sensitive-enhanced, sensitive, and critical applications and information resources that are part of the Postal Service infrastructure must meet or exceed the requirements documented in the Postal Service's configuration baseline. During our review, we did not identify any approved deviations from the IV configuration baseline.

The Enterprise Computing [redacted] Engineering Team stated that these misconfigurations existed because system administrators did not validate the configurations when they updated the servers. As a result, [redacted] hese insecure settings could impact the confidentiality, integrity, and availability of all the IV servers because the operating system configurations are all created from the standard configuration builds.

In addition, while comparing the [redacted] Configuration Baseline to industry benchmarks,[8] we identified 76 of 221 recommended security settings from the Center for Internet Security (CIS)[9] SUSE[10] benchmark and 74 of 226 settings from the CIS Red Hat benchmark that were not included in the Postal Service's baseline document. See Appendix B for descriptions of the specific settings.

According to Postal Service policy[11], information security policies, procedures, and standards are developed to support an enterprise information security program that meets federal requirements and incorporates industry practices. These industry IT security benchmarks guide the IT community in safeguarding operating systems, software, and networks that are most vulnerable to cyber-attacks. Inclusion of current and applicable controls from IT security industry leaders strengthen the security posture of the IV system and operations.

Recommendation #1

Vice President, Information Technology, develop a process to ensure that Informed Visibility server configurations comply with the established configuration baseline.

Recommendation #2

Vice President, Information Technology, review the controls identified in the Center for Internet Security benchmarks and consider them for inclusion into the published standard.

2 [redacted] *Configuration Baseline*, April 2, 2018.

3 The U.S. Postal Service Office of Inspector General (OIG) selected a non-statistical sample and compared 13 of the 96 externally-facing and supporting IV servers to the configuration baseline. [redacted]

9 CIS benchmarks are consensus-based guides curated by security practitioners.

11 *Administrative Support Manual*, Issue 13, Section 862.14, Information Security Policies, Procedures, and Standards, July 1999 updated through October 26, 2017.

Finding #2: Web Application Encryption and Authentication

Overall, the IV web application encryption and authentication were secure. However, we identified three encryption and authentication vulnerabilities related to communication protocols. Industry standards recommend that all web applications use the latest improved protocol version that provides a stronger encryption and authentication capability.[12] Specifically, we identified the vulnerabilities outlined in Table 1.

Table 1: Identified Web Application Vulnerabilities

Severity Level	Vulnerability
Critical	[redacted]
High	[redacted]
Medium	[redacted]

Source: OIG HP WebInspect scan results.

This occurred because these communication protocols were not identified for upgrade in the Postal Service's IV web application configuration review. The web application encryption and authentication protocol vulnerabilities we identified would allow an attacker to [redacted]. Implementing the latest version of data encryption and authentication protocols help protect the confidentiality and integrity of the IV system and the data transmitted between its clients and web server. Management took corrective action to remediate all three vulnerabilities by upgrading to the latest version of TLS (1.2) and disabled support for TLS 1.0 and 1.1.

> *"Overall, the IV web application encryption and authentication were secure."*

Recommendation #3

Vice President, Enterprise Analytics, include communication protocols in future Informed Visibility web application configuration reviews and address any control weaknesses identified.

Finding #3: [redacted] Database Account Management and Audit Logging

Although [redacted] databases were recently incorporated into the IV environment, the Postal Service has not implemented required account management controls and not enabled audit logging for them.

Account Management. While the [redacted] databases we reviewed provided limited account management functionality, these databases currently do not have the capability to fully implement Postal Service user account management requirements. As a result, the Postal Service [redacted]

Management recognizes that account management is an issue and plans to integrate the [redacted] databases with [redacted] by the end of 2018.

12 NIST Special Publication 800-52, rev. 1, *Guidelines for the Selection, Configuration, and Use of Transport Layer Implementations*, April 2014, recommends that all web applications use the latest version of TLS (version 1.2).

[redacted]

14 The Customer Registration application serves as the single-sign on entry for all business clients to other Postal Service online applications.

15 Handbook AS-805, Sections 9-5.3, Suspending Log-on IDs and 9-6.1.1, Password Selection Requirements, February 2018.

16 Handbook AS-805, Section 9-6.1.1, Password Selection Requirements states that passwords must consist of at least 15 characters and contain at least one character from three of the four following types of characters: English uppercase letters (A–Z), English lowercase letters (a–z), Westernized Arabic numerals (0–9), and non-alphanumeric characters (i.e., special characters such as &, #, and $).

[redacted]

Audit Logging. The IV [redacted] databases are not set to perform audit logging to capture database events and management has not formally accepted the risk. Postal Service policy[17] also states that all information resources including databases must implement system-level audit logging. According to management, this was not set because enabling audit logging to capture database events degraded system performance. However, audit logging may be enabled pending the results of future system performance assessments. Without audit logs, the Postal Service [redacted]

Recommendation #4

Vice President, Enterprise Analytics, and Vice President, Information Technology, implement account management controls for the Informed Visibility [redacted] databases to meet Postal Service requirements.

Recommendation #5

Vice President, Enterprise Analytics, and Vice President, Information Technology, enable the audit logging function for the Informed Visibility [redacted] databases or approve a risk acceptance letter.

Finding #4: [redacted] Configuration Baseline

The Postal Service has not fully developed a configuration baseline for the IV [redacted] databases. Postal Service policy[18] requires hardware and system software to be hardened to Postal Service information security requirements and databases not be deployed to a production environment prior to hardening. The IV system was certified, accredited, and deployed to a production environment in 2014 and recertified in February 2017. The Postal Service began using the [redacted] databases in production without a configuration baseline.

According to Postal Service management, this occurred because [redacted] was the first iteration of a Not Only Structured Query Language (NoSQL)[19] database and management was not aware they needed to create a configuration baseline. In 2018, management drafted a configuration baseline to address this requirement.

> *"The Postal Service has not fully developed a configuration baseline for the IV [redacted] databases."*

Without a configuration baseline, management [redacted] the IV system.

Recommendation #6

Vice President, Information Technology, Vice President, Chief Information Security Officer, and the Vice President, Enterprise Analytics, finalize, publish, and implement the [redacted] database configuration baseline document.

17 Handbook AS-805, Section 9-11, February 2018.

[redacted]

19 NoSQL is a non-relational database that stores and accesses data. Instead of storing data in rows and columns like a traditional database, NoSQL is used to store each item individually with a unique key.

Other Matter: Multiple Operating System Configuration Documents

During our audit, we identified a matter that did not rise to the level of a finding. However, we wanted to make management aware of the risk of a version control issue with the [redacted] operating system configuration documents. We found the Postal Service maintains two separate documents containing the [redacted] operating system configurations. Since both are maintained on Postal Service's official repository, there is confusion as to which document should be implemented. Management provided the OIG with both documents as the official configuration baseline for the IV system.

> *"We found the Postal Service maintains two separate documents containing the [redacted] operating system configurations."*

- The Enterprise Computing [redacted] Engineering Team provided the OIG with the [redacted] Configuration Baseline document,[20] which contains both [redacted] and [redacted] operating system configurations. The [redacted] Configuration Baseline document is the approved document used for all Postal Service compliance testing for the IV servers.
- The Corporate Information Security Office provided the OIG with the [redacted] document,[21] which is posted on the Postal Service's portal[22] as official documentation. However, this document is not included in the approved Postal Service configuration settings.

Postal Service policy requires management of its paper and online documents so that they are correct, up-to-date, easy to find, and in agreement with official Postal Service policies and procedures.[23] We do not consider this to be a finding because these documents do not significantly differ now; however, there is the risk that the two documents may diverge moving forward and contain different configuration setting information.

Management's Comments

Management agreed with two of the six recommendations in the report. Management agreed with recommendations 1 and 5 and disagreed with recommendations 2, 3, 4, and 6.

Regarding recommendation 1, management stated that they developed processes in June 2018 to comply with the configuration baselines and eliminate the identified risks through defense in-depth concepts. No target implementation date was provided.

Regarding recommendation 2, management stated that there is a process in place to develop standards, which includes controls from a variety of industry internet security benchmark sources in the completed published standard. The Postal Service employs the Center for Internet Security as one of several sources for hardening guidelines.

Regarding recommendation 3, management stated that the Postal Service's internet accessible applications utilize a variety of techniques to ensure their security, including TLS protocol. The TLS upgrade was completed in June 2018 during our audit.

Regarding recommendation 4, management stated that the security layers combined with limited account management capabilities support the policies of least privilege and separation of duties. Postal Service personnel with [redacted] database access have appropriate privilege and are restricted to the appropriate access level.

Regarding recommendation 5, management will continue to work with the vendor to incorporate audit logging when future enhancements are made that do not impact system performance. Management will document the risks, workarounds,

[redacted]

22 Approved Configuration Baseline document contained in the Corporate Information Security Hardening Standards Repository.
23 Management Instruction AS-310-2013, *Management of Policy and Procedure Information*, June 26, 2013.

and future planning concerning audit logging. The target implementation date is December 2018.

Regarding recommendation 6, management stated that the [redacted] database baseline document configurations are identified and stored in a version control system where they can be retrieved and deployed as part of the automatic build processes.

Evaluation of Management's Comments

The OIG considers management's comments partially responsive to recommendation 5 and non-responsive to recommendations 1, 2, 3, 4, and 6.

Regarding recommendation 1, management stated that they developed a process to ensure that Informed Visibility server configurations comply with the established configuration baseline. While management agreed with our finding, they have not provided the OIG any evidence or a target implementation date that supports their efforts to develop a process to comply with the established baseline.

Regarding recommendation 2, management stated that they review the controls identified in the Center for Internet Security benchmarks and consider them for inclusion into the published standard. Management has not provided the OIG with any evidence that supports their review of the benchmarks and their justifications for exclusion. Inclusion of current and applicable controls from IT security industry leaders strengthens the security posture of system and operations.

Regarding recommendation 3, management stated they would include communication protocols in future IV web application configuration reviews and address any control weaknesses identified. Management took corrective action by upgrading the TLS protocol specifically identified as a result of our review. However, management has not provided the OIG with any official documentation showing inclusion of the protocols for future IV web application configuration review. Implementing the latest version of data encryption and authentication protocols helps protect the confidentiality and integrity of systems.

Regarding recommendation 4, management stated account management controls for the IV [redacted] databases were in place to meet Postal Service requirements. Management's response does not address the specific controls identified in th report. Although management disagreed with the recommendation, during the audit they recognized account management is an issue and plans to integrate the [redacted] databases with [redacted] by the end of 2018. Management has not provided evidence to support resolution of the issues addressed in the report.

Regarding recommendation 5, management stated their commitment to work with the vendor to incorporate audit logging for the [redacted] database; however, management did not commit to approving a risk acceptance letter if system performance prevents it.

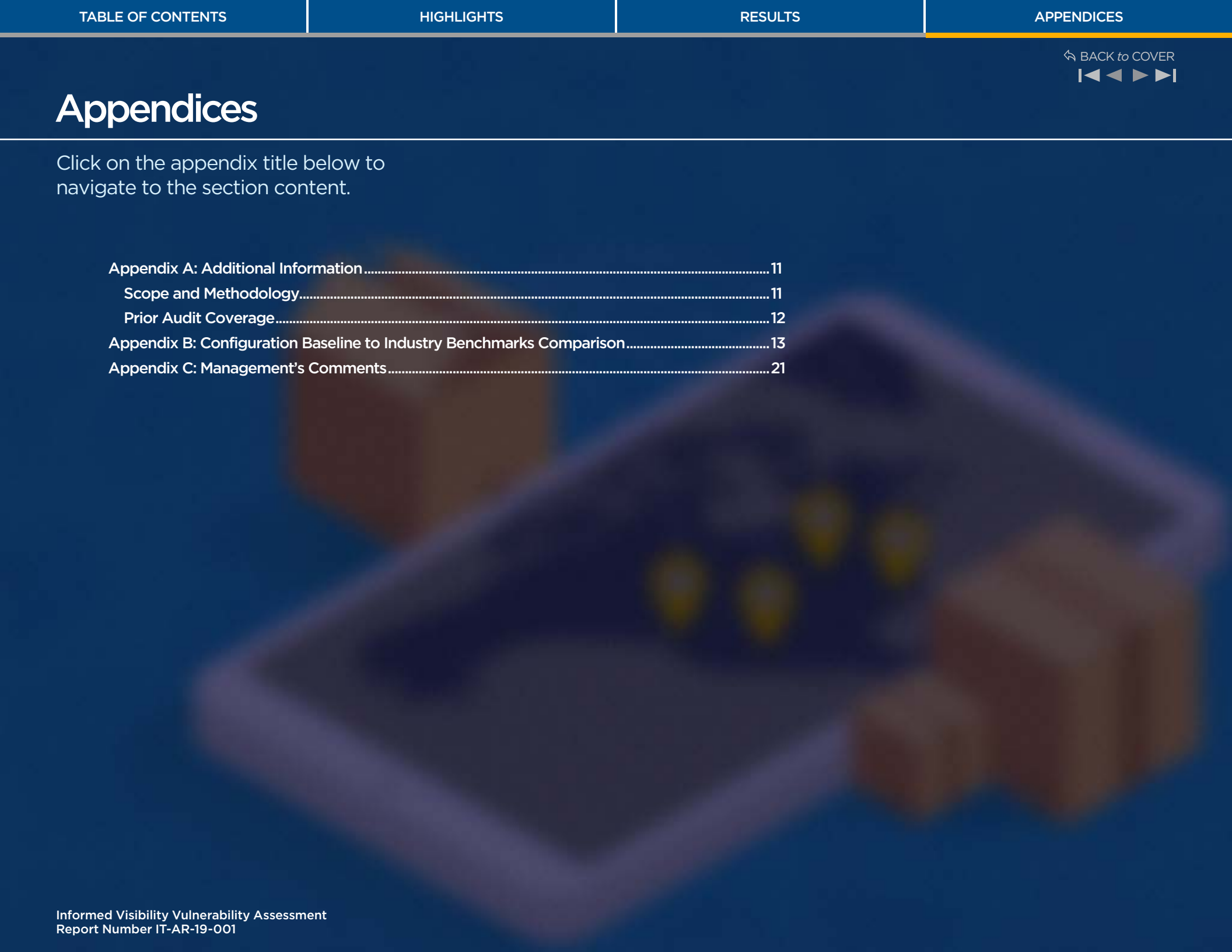
Regarding recommendation 6, management stated that baseline document configurations are identified and stored in a version control system that can be retrieved as part of the automatic build process. Although management disagreed with this recommendation in their response, during the audit they drafted a configuration baseline to address this requirement. However, the OIG has not been provided with a final approved version of this document.

Management also stated in their general comments that the report contains an inaccurate IV deployment date. The OIG provided the start date of their initial deployment activities (i.e., November 2014), as documented in the Postal Service's "Exhibit D: Revised Project Schedule".

All recommendations require OIG concurrence before closure. Consequently, the OIG requests written confirmation when corrective actions are completed. For recommendations where management disagreed with the recommended corrective action, the OIG will pursue formal audit resolution. No recommendations should 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

The OIG conducts security vulnerability assessments to ensure that Postal Service computer systems provide an appropriate security level commensurate with the criticality of the system and the information contained on the system. The tools used to perform the vulnerability scans are HP WebInspect and Nessus®.

- HP WebInspect is 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.
- Nessus is a vulnerability and configuration assessment product that features high-speed discovery, configuration auditing, asset profiling, sensitive data discovery, patch management integration, and vulnerability analysis.

The scope of our audit was the externally-facing and supporting IV web application, databases, and servers. The feeder systems that supply data to IV were not in our scope.

To accomplish our objective, we:

- Reviewed Postal Service policies and best practices relevant to the IV operating system, databases, and web applications to configure our scanning tools and reconcile our results.
- Extracted and reviewed data for the servers and databases comprising the IV system from network diagrams and Advanced Configuration Management Database (CMDB) Reporting Service (ACRS)[24]. We used this information to identify the system attributes, Internet protocol address subnet ranges, asset inventory, and other relevant information.
- Performed automated scans using Nessus and HP WebInspect from March 12 through March 16, 2018, and analyzed scan results to Postal Service policies and industry best practices, assessing compliance and identifying vulnerabilities.
- Selected a non-statistical sample of 13 SUSE and Red Hat servers and conducted a manual review to determine compliance with Postal Service baseline configurations.
- Compared the Postal Service Information Technology organization's [redacted], to the Center for Internet Security's *Red Hat Enterprise* [redacted] and [redacted] benchmarks.
- Leveraged advanced techniques to analyze data using tools to include Perl, MySQL, and Microsoft Excel to generate our results. Based on our analysis, we determined the severity ranking and Common Vulnerabilities and Exposures and mapped them to the Confidentiality, Integrity, and Availability Triad.
- Interviewed Postal Service management regarding the [redacted] databases and reviewed relevant documentation.
- Conducted interviews and provided the data analysis results to appropriate Postal Service management to determine control deficiencies in the IV servers and to identify the root cause and compensating controls for confirmed vulnerabilities.

We conducted this performance audit from October 2017 through October 2018, 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 the

24 ACRS is front-end reporting service for the Atrium CMDB and the Postal Service's IT environment. It is driven by a combination of auto-discovered and manually provided IT configuration data of IT assets.

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 August 27, 2018, and included their comments where appropriate.

We did not assess the reliability of any computer-generated data 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: Configuration Baseline to Industry Benchmarks Comparison

The following table details 76 recommended security settings from the CIS [redacted] benchmark not included in the Postal Service's [redacted] Configuration Baseline.

CIS [redacted] Recommended Security Settings		
	Section	Configuration
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]

CIS [redacted] Recommended Security Settings		
	Section	Configuration
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

CIS [redacted] Recommended Security Settings		
	Section	Configuration
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

CIS [redacted] Recommended Security Settings	
Section	Configuration
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

Source: OIG comparison results.

The following table details 74 recommended security settings from the CIS Red Hat Enterprise [redacted] benchmark not included in the Postal Service's [redacted] Configuration Baseline.

CIS Red Hat Enterprise [redacted] Recommended Security Settings	
Section	Configuration
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

CIS Red Hat Enterprise [redacted] Recommended Security Settings		
	Section	Configuration
☐	[redacted]	[redacted]
☐	[redacted]	[redacted]
☐	[redacted]	[redacted]
☐	[redacted]	[redacted]
☐	[redacted]	[redacted]
☐	[redacted]	[redacted]
☐	[redacted]	[redacted]
☐	[redacted]	[redacted]
☐	[redacted]	[redacted]
☐	[redacted]	[redacted]
☐	[redacted]	[redacted]
☐	[redacted]	[redacted]
☐	[redacted]	[redacted]
☐	[redacted]	[redacted]
☐	[redacted]	[redacted]
☐	[redacted]	[redacted]
☐	[redacted]	[redacted]
☐	[redacted]	[redacted]
☐	[redacted]	[redacted]
☐	[redacted]	[redacted]
☐	[redacted]	[redacted]
☐	[redacted]	[redacted]
☐	[redacted]	[redacted]
☐	[redacted]	[redacted]

CIS Red Hat Enterprise [redacted] Recommended Security Settings		
	Section	Configuration
☐	[redacted]	[redacted]
☐	[redacted]	[redacted]
☐	[redacted]	[redacted]
☐	[redacted]	[redacted]
☐	[redacted]	[redacted]
☐	[redacted]	[redacted]
☐	[redacted]	[redacted]
☐	[redacted]	[redacted]
☐	[redacted]	[redacted]
☐	[redacted]	[redacted]
☐	[redacted]	[redacted]
☐	[redacted]	[redacted]
☐	[redacted]	[redacted]
☐	[redacted]	[redacted]
☐	[redacted]	[redacted]
☐	[redacted]	[redacted]
☐	[redacted]	[redacted]
☐	[redacted]	[redacted]
☐	[redacted]	[redacted]
☐	[redacted]	[redacted]
☐	[redacted]	[redacted]
☐	[redacted]	[redacted]
☐	[redacted]	[redacted]
☐	[redacted]	[redacted]
☐	[redacted]	[redacted]
☐	[redacted]	[redacted]

CIS Red Hat Enterprise [redacted] Recommended Security Settings	
Section	Configuration
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

CIS Red Hat Enterprise [redacted] Recommended Security Settings		
	Section	Configuration
☐	[redacted]	[redacted]
☐	[redacted]	[redacted]
☐	[redacted]	[redacted]
☐	[redacted]	[redacted]

Source: OIG comparison results.

Appendix C: Management's Comments

UNITED STATES POSTAL SERVICE

September 20, 2018

MONIQUE COLTER
DIRECTOR, AUDIT OPERATIONS

SUBJECT: Informed Visibility Vulnerability Assessment, Report Number IT-AR-18-DRAFT

Thank you for the opportunity to review and comment on the Office of Inspector General (OIG) Audit of Informed Visibility Vulnerability Assessment. Our comments on the draft report and our responses to the OIG Recommendations are set forth below.

General Comments:

This audit recognizes that the Postal Service complies with Postal Service security control requirements and industry best practices for the externally-facing and supporting IV servers and databases.

However, there are some inaccuracies in the timeline pertinent to IV Development/ Deployment effort. It should be noted that the Postal Service deployed IV Internal SPM in October 2015 and implemented the Enterprise [redacted] database management system in IV in February 2017.

In addition, the Postal Service disagrees that the recommendations will strengthen the risk postures of confidentiality, integrity or availability of the Informed Visibility system. USPS considers information security critically important and Postal Systems apply multiple depth layers of defense to help ensure security of its applications.

Recommendation [1]:
Vice President, Information Technology, develop a process to ensure that Informed Visibility server configurations comply with the established configuration baseline.

Management Response/Action Plan
Management agrees with recommendation 1 and its associated risk profile. To address this, the Postal Service developed processes in June, 2018 to comply with configuration baselines and eliminates the identified risks through defense in depth concepts.

Target Implementation Date:
N/A

Recommendation [2]:
Vice President, Information Technology, review the controls identified in the Center for Internet Security benchmarks and consider them for inclusion into the published standard.

Management Response/Action Plan
Management disagrees with recommendation 2 as there is a process in place to develop standards which include controls from a variety of industry internet security benchmark sources in the completed published standard. The Postal Service employs the Center for Internet Security as one of several sources for hardening guidelines.

Page 1 of 4

Target Implementation Date:
N/A

Recommendation [3]:
Vice President, Enterprise Analytics, include communication protocols in future IV web application configuration reviews and address any control weaknesses identified.

Management Response/Action Plan
Management disagrees with recommendation 3. The Postal Service's internet accessible applications utilize a variety of techniques to ensure their security including TLS protocol. Based on an OIG Audit finding, TLS upgrades and other security upgrades are implemented on a regular basis for systems. The TLS upgrade was completed in June 2018 while the Audit was being conducted.

Target Implementation Date:
N/A

Recommendation [4]:
Vice President, Enterprise Analytics, and Vice President, Information Technology, implement account management controls for the IV [redacted] databases to meet Postal Service requirements.

Management Response/Action Plan
Management disagrees with recommendation 4. The security layers combined with limited account management capabilities support the policies of least privilege and separation of duties. Postal Service personnel with [redacted] database access have appropriate privilege and are restricted to the appropriate access level.

Target Implementation Date:
N/A

Recommendation [5]:
Vice President, Enterprise Analytics, and Vice President, Information Technology, enable the audit logging function for the IV [redacted] databases or approve a risk acceptance letter.

Management Response/Action Plan
Management agrees with recommendation 5. The ability to generate these logs without impacting performance is a technical issue that as the [redacted] technology improves will allow the Postal Service to collect logging. USPS views this as low risk due to the defense in depth layers of security that Postal Systems deploy in the network and hosting tiers that would enable Postal Service to reconstruct activities in the event of a compromise or malfunction of all except the internal [redacted] database activities. The Postal Service will continue to work with the vendor to incorporate audit logging when future enhancements are made that do not impact performance. The Postal Service will document the risks, workarounds, and future planning.

Target Implementation Date:
December 2018

Responsible Official:
Vice President, Enterprise Analytics and Vice President, Information Technology

Recommendation [6]:
Vice President, Information Technology, Vice President, Chief Information Security Officer, and the Vice President, Enterprise Analytics, finalize, publish, and implement the [redacted] database configuration baseline document.

Page 2 of 4

Management Response/Action Plan
Management disagrees with recommendation 6. The [redacted] database baseline document configurations are identified and stored in a version control system where they can be retrieved and deployed as part of automatic build processes.

Target Implementation Date:
N/A

Isaac Cronkhite
Vice President, Enterprise Analytics

Jeffrey Johnson
Vice President, Information Technology

Recoverable Signature

X

Lisa Holman
Deputy CISO
Signed by: lcholman@uspis.gov

for
Gregory S. Crabb
Vice President, Chief Information Security Office

Page 3 of 4

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