Security Assessment of a U.S. Postal Service Product Solutions Application

AUDIT REPORT

Report Number 22-197-R24 | December 8, 2023

Table of Contents

Highlights

Background

The U.S. Postal Service continuously strives to improve its [redacted] to become more efficient and responsive to the dynamic market needs of its customers. To [redacted] application is used by over [redacted] is a business-critical application that generated over [redacted] total revenue in fiscal year 2022.

What We Did

Our objective was to evaluate whether the Postal Service had security controls in place to protect the [redacted] application from cyberattacks, prevent unauthorized access to restricted data, and determine compliance with secure coding practices. We conducted a security assessment of the [redacted] application including penetration tests to evaluate the [redacted] application and internal security posture. We also performed a source code review to verify if appropriate security controls were present.

What We Found

Based on our testing, we found the Postal Service implemented network perimeter security controls that limit direct access to the application and help deter known web-based attacks. However, during our security assessment, we identified issues with [redacted]. These issues could lead to attackers gaining unauthorized access to the system to steal, modify, or delete sensitive [redacted] data if perimeter controls are bypassed. These issues occurred because management did not [redacted] Also, the Postal Service prioritizes the identification and remediation of vulnerabilities ranked critical and high over medium, low, and informational. However, [redacted], increases the risk of unauthorized access to the application. In addition, [redacted]

Recommendations

We recommended management develop guidance for performing [redacted] application; and [redacted].

Transmittal Letter

OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

December 8, 2023

MEMORANDUM FOR: WILLIAM E. KOETZ, VICE PRESIDENT, NETWORK & COMPUTE TECHNOLOGY

HEATHER L. DYER, VICE PRESIDENT, CHIEF INFORMATION SECURITY OFFICER

ANGELA D. LAWSON, VICE PRESIDENT, TECHNOLOGY APPLICATIONS

FROM: Wilvia Espinoza
Deputy Assistant Inspector General
for Inspection Service, Technology, and Services

SUBJECT: Audit Report – Security Assessment of a U.S. Postal Service Product Solutions Application (Report Number 22-197-R24)

This report presents the results of our Security Assessment of a U.S. Postal Service Product Solutions Application audit.

We appreciate the cooperation and courtesies provided by your staff. If you have any questions or need additional information, please contact Vasilios Grasos, Director, Cyber Security & Technology Directorate, 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 Security Assessment of a U.S. Postal Service Product Solutions Application (Project Number 22-197). Our objective was to evaluate whether the U.S. Postal Service had security controls in place to protect the [redacted] application from cyberattacks and prevent unauthorized access to restricted data, and to determine compliance with secure coding practices. See Appendix A for additional information about this audit.

Background

The Postal Service continuously strives to improve its [redacted] to become more efficient and responsive to the dynamic market needs of its customers and create services and features that enhance the value of the mail. To expedite [redacted] The [redacted] application provides the following features:

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

[redacted]

[redacted] is a business-critical application that generated over [redacted] in total revenue in fiscal year 2022.[6] The application development team, which falls under the Technology Applications group, developed and regularly modifies the [redacted] application, to include designing and coding software according to Postal Service's security requirements[7] in all phases of the software development life cycle.

The Chief Information Security Office (CISO) conducts vulnerability assessments weekly and penetration tests as needed of the [redacted] application to identify and coordinate the remediation of vulnerabilities. When vulnerabilities are identified, the CISO Vulnerability Remediation Management team leverages several data sources to prioritize the vulnerabilities, identifies appropriate stakeholders, initiates a campaign to address the highest priority vulnerabilities, and tracks them through completion. For the penetration test, the CISO Penetration Testing team creates incident tickets, sends results to the application owners, and tracks and validates the remediation.

The Network Compute & Technology (NCT) team is one of the stakeholders who is responsible for remediating [redacted] operating system and database vulnerabilities identified by CISO. They also assist the application development team with deploying updates to the application.

To evaluate the security controls of the [redacted] Application, we conducted a comprehensive security assessment that included:

- Penetration testing – an assessment of a network or web application to discover vulnerabilities

1 USPS Enterprise Data Warehouse, June 2023.
2 [redacted]
3 Data obtained from USPS Enterprise Data Warehouse, June 2023 and [redacted] (usps.gov).
4 [redacted]
5 USPS.com [redacted], July 2023.
6 USPS Enterprise Data Warehouse, June 2023.
7 [redacted]

and security weaknesses.[8] Penetration testing involves testers using controlled attack methods to simulate hackers. These tests are also used to validate the effectiveness of defensive methods and adherence to security policies.

- Source code review – a manual or automated review of an application's source code to identify poor coding practices and security weaknesses related to its design or features. Reviewing the source code allows organizations to determine if the application meets secure coding practices and has effective controls against attacks.

These assessments are designed to check for common vulnerabilities within the application that could potentially be exploited. Vulnerabilities are ranked as critical, high, medium, low, and informational, based on the ease and impact of an attacker exploiting the vulnerability. Common vulnerabilities are based on industry standard rankings that include the type of issue and results of those issues. Some of the common vulnerabilities include:

- Injection – when user supplied data is not validated, filtered, or sanitized by the application.
- Security Misconfigurations – when there are missing security parameters; unnecessary features are enabled or installed; or security settings are not set to secure values in the application servers, framework libraries, or databases.
- Vulnerable and Outdated Components – when software has a security flaw, is unsupported, or is out of date. This includes if the operating system, web/application server, databases, or the underlying platform is not fixed or upgraded timely. This commonly happens in environments when security patching is a monthly or quarterly task, leaving organizations open to days or months of unnecessary exposure to vulnerabilities with known fixes.

Findings Summary

Based on our testing, we found the Postal Service implemented network perimeter security controls that limit direct access to the application and help deter known web-based attacks. However, during our security assessment, we identified issues with [redacted]

Finding #1: Penetration Test Results

During our external and internal penetration test of the [redacted] application, we found that CISO and NCT implemented a content [redacted] However, our testing found the application was not [redacted] We also found [redacted] that, if exploited, could leave the system vulnerable (see Table 1).

8 Cybersecurity and Infrastructure Security Agency, Penetration Testing Fundamentals, August 16, 2022.
9 [redacted]
10 [redacted]
11 [redacted]
12 [redacted]
13 [redacted]
14 [redacted]

Table 1. Penetration Test Results

Vulnerability Type	Vulnerability	Instances	Risk Factor
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

Source: Penetration testing tool results.

[redacted]

We found [redacted] vulnerabilities in the [redacted] application that could allow an attacker to [redacted] the application. Postal Service policy states that [redacted] However, we identified:

- [redacted] instances associated with [redacted] vulnerabilities that could [redacted]
- [redacted] instances of a vulnerability [redacted] and
- [redacted] instances of a vulnerability that [redacted]

[redacted]

[redacted]

The Postal Service did not always ensure [redacted] Specifically, we found:

- [redacted] instances of a [redacted]

Postal Service policy states that sensitive data must be [redacted] When the [redacted] (see Figure 1).

15 [redacted]
16 [redacted]

Figure 1.

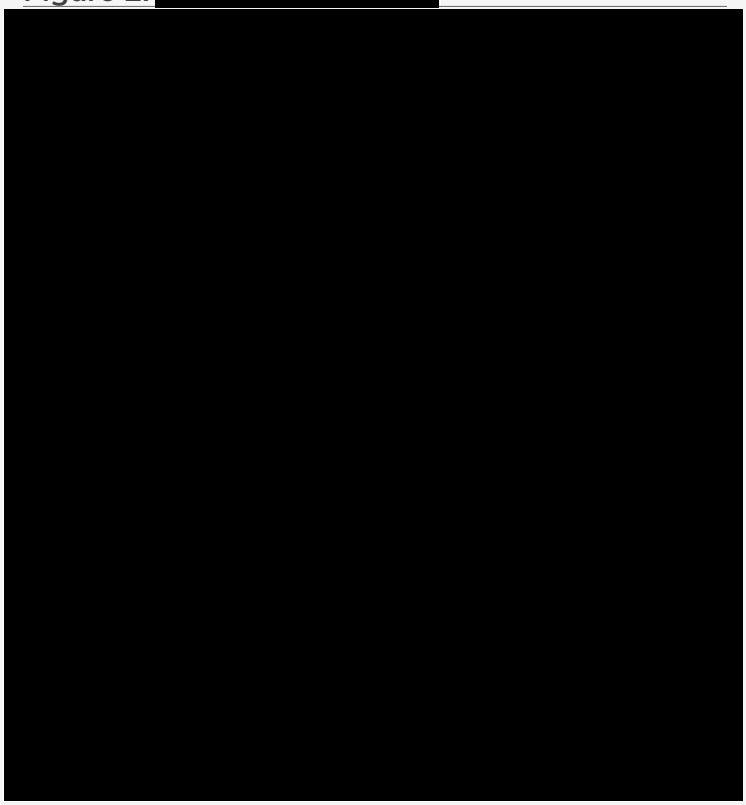
Source: USPS OIG Illustration.

We found instances where Postal Service policy states that all applications using We also found instances where This increases the risk of an attacker Postal service policy prohibits Finally, there were instances where Best practices state that

We also found vulnerabilities that, , could be leveraged by an attacker Specifically, we identified instances of as well as instances of Although these vulnerabilities were respectively,[21] This type of attack occurs when This method of attack can be used (see Figure 2).

17
18
19
20
21

Figure 2. [redacted]



Source: USPS OIG Illustration.

Postal Service policy requires the use [redacted] By leveraging the [redacted] For example, we were able to [redacted]

These issues occurred, in part, because according to CISO management, [redacted] The application development team did not [redacted] Further, a penetration test [redacted]

[redacted]

Additionally, the application development team stated that [redacted] Although the CISO provides all vulnerability [redacted] However, [redacted] especially if they can [redacted] increases the risk of unauthorized access to the [redacted] application.

Recommendation #1

We recommend the **Vice President, Chief Information Security Officer,** develop guidance to identify the criteria and minimum frequency for [redacted]

Recommendation #2

We recommend the **Vice President, Chief Information Security Officer, Vice President, Network & Compute Technology,** and **Vice President, Technology Applications,** develop a plan of action and milestones to [redacted] application.

Recommendation #3

We recommend the **Vice President, Chief Information Security Officer, Vice President, Network & Compute Technology,** and **Vice President, Technology Applications,** develop a plan to review medium, low, and informational vulnerabilities that could impact the [redacted] application and remediate these vulnerabilities, as appropriate.

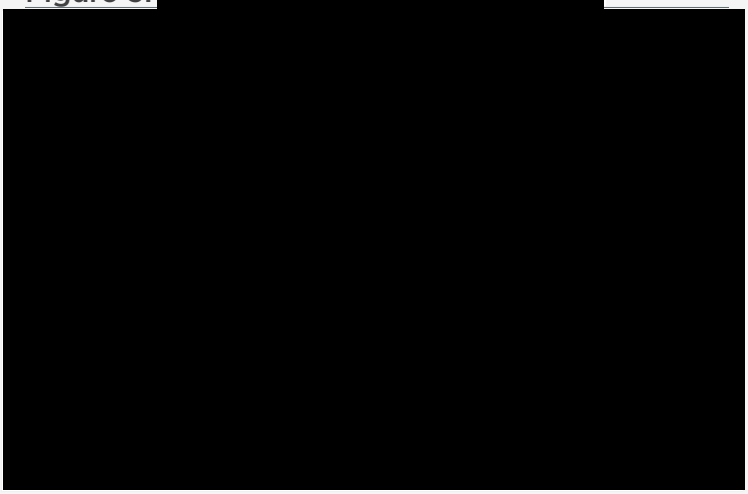
Finding #2: [redacted]

During our [redacted] review, we found that the [redacted] application development team did not always follow Postal Service [redacted] Specifically, we found issues with [redacted]

22 [redacted]
23 [redacted]
24 [redacted]

[redacted] (see Figure 3).

Figure 3. [redacted]



Source: USPS OIG Illustration.

Postal Service policy states that sensitive information, such as [redacted] These issues could allow a malicious user unauthorized access to sensitive information.

[redacted] We found [redacted] instances in which the [redacted] did not [redacted] Postal Service policy states that [redacted] can lead to attackers [redacted]

We found that the [redacted] developers did not always [redacted] in accordance with policy. We found [redacted] instances of [redacted] in the [redacted] application [redacted] This could allow application [redacted] For example, this could cause the application to [redacted] Postal Service policy states that [redacted] (see Figure 4).

Figure 4. [redacted]

Source: [redacted] Review Results.

25 [redacted]
26 [redacted]
27 [redacted]
28 [redacted]

[redacted]

We found that the [redacted] application did not always [redacted] Specifically, we found that data was not [redacted] This can lead to [redacted] As a result of our audit, management took corrective action and remediated this vulnerability by [redacted]

We found that the Postal Service did not always [redacted] in accordance with policy. Specifically, [redacted] Postal Service policy states that all [redacted] which could increase the risk of unauthorized access to sensitive data.

Management stated that all [redacted] Management also stated that [redacted] While management was aware of the [redacted] they prioritized other work such as [redacted] However, best practices state that [redacted]

[redacted]

Recommendation #4

We recommend the **Vice President, Technology Applications,** [redacted]

Management's Comments

Management agreed with finding 1; disagreed with finding 2; agreed with recommendations 1, 2, and 3; and partially agreed with recommendation 4.

Regarding finding 2, management stated [redacted] They also stated that [redacted]

Regarding recommendation 1, management stated the CISO Scanning and Vulnerability Assessment team will work with [redacted] stakeholders to determine criteria and minimum frequency for [redacted]. The target implementation date is November 30, 2024.

Regarding recommendation 2, management stated they will create a plan to [redacted] as defined in the [redacted] Playbook. The target implementation date is March 29, 2024.

Regarding recommendation 3, management stated they will review reports provided by CISO to prioritize and develop a plan to resolve medium, low, and informational findings for the [redacted] application. The target implementation date is March 29, 2024.

Regarding recommendation 4, management stated they will [redacted] Management further stated [redacted] The target implementation date is April 15, 2024.

29 [redacted]
30 [redacted]
31 [redacted]
32 [redacted]
33 [redacted]

See Appendix B for management's comments in their entirety.

Evaluation of Management's Comments

The OIG considers management's comments responsive to recommendations 1, 2, and 3 and generally responsive to recommendation 4. The actions planned to address these recommendations should resolve the issues identified in the report.

Regarding recommendation 4, during our audit, management stated that the issues we identified were associated wit [redacted] Management stated it would [redacted] which would satisfy the intent of this recommendation.

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.

Appendices

Appendix A: Additional Information

Scope and Methodology

We conducted a comprehensive security assessment of the [redacted] application. Our penetration test scope included servers, databases, and network devices that support the application. The [redacted] For our review we judgmentally selected [redacted] based on the [redacted] and the high likelihood or ease in which [redacted]

We conducted audit work at the [redacted]

Our methodology included a comprehensive security assessment to identify security weaknesses and verify that adequate controls were in place and working as intended. This security assessment consisted of an:

- External penetration test from May 30 to June 8, 2023, and an internal penetration test from June 13 to June 22, 2023, and July 18 to July 20, 2023.
- Source code review from May 30, 2023, to June 15, 2023.

In addition, we:

- Interviewed the appropriate personnel to gain an understanding of the Postal Service's security assessments.
- Reviewed policies, procedures, and best practices to determine the security requirements and secure development practices related to penetration testing and source code reviews.
- Coordinated with the Postal Service to develop a "Rules of Engagement/Technical Assessment Plan" that identified and documented the approved guidelines for the penetration tests and secure code review.
- Leveraged manual and automated techniques and tools to gather [redacted] application information and assess the application and supporting infrastructure.

We conducted this performance audit from November 2022 through December 2023 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 November 8, 2023, and included their comments where appropriate.

In planning and conducting the audit, we obtained an understanding of the [redacted] application internal control structure to help determine the nature, timing, and extent of our audit procedures. We reviewed the management controls for overseeing the program and mitigating associated risks. Additionally, we assessed the internal control components and underlying principles, and we determined that the following two components were significant to our audit objective: risk assessment and control activities.

We developed audit work to ensure that we assessed these controls. Based on the work performed, we identified internal control deficiencies related to control activities that were significant within the context of our objectives. Our recommendations, if implemented, should correct the weaknesses we identified.

We assessed the reliability of computer-generated data that resulted from our automated testing by analyzing and reviewing the raw data, performing manual and automated reconciliations 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
Security Assessment of [redacted]	To evaluate the U.S. Postal Service's security controls in place to protect the [redacted] application from cyberattacks and prevent unauthorized access to restricted data.	20-286-R21	9/9/2021	N/A
Security Assessment of a U.S. Postal Service Information Technology Application	To determine if the U.S. Postal Service has effective security controls to protect [redacted] from cyberattacks and prevent unauthorized access to restricted data.	19-018-R20	8/11/2020	N/A
Review of Postal Service's Response to an Identified Security Weakness	To determine if the U.S. Postal Service appropriately responded to and mitigated an identified security weakness affecting the [redacted] application.	19TG005IT000	9/6/2019	N/A

Appendix B: Management's Comments

UNITED STATES POSTAL SERVICE

Date: December 1, 2023

JOHN CIHOTA
DIRECTOR, AUDIT SERVICES

SUBJECT: Management Response: Security Assessment of a U.S. Postal Service Product Solutions Application 22-197

Thank you for providing the Postal Service with an opportunity to review and comment on the findings and recommendations contained in the draft audit report *Security Assessment of a U.S. Postal Service Product Solutions Application*

Finding 1: **Penetration Test Results**
During our external and internal penetration test of the [redacted] application, we found that CISO and NCT implemented [redacted] However, our testing found the application was not [redacted] We also found [redacted] that, if exploited, could leave the [redacted] system vulnerable.

Management Response:
Management agrees with this finding.

Finding 2: [redacted]
During our [redacted] review, we found that the [redacted] application development team did not always follow Postal Service [redacted] Specifically, we found issues with [redacted]

Management Response:
Management disagrees that the development teams do not following [redacted] follows USPS [redacted] for all releases. The [redacted]

Recommendation 1:
We recommend the **Vice President, Chief Information Security Officer,** develop guidance to identify the criteria and minimum frequency for [redacted]

Management Response/Action Plan:
Management agrees with this recommendation. The CISO Scanning and Vulnerability Assessments (SVA) team will work with stakeholders from the [redacted] Team to determine

appropriate criteria and minimum frequency for [redacted]

Target Implementation Date:
November 30, 2024

Responsible Official:
Vice President, Chief Information Security Officer

Recommendation 2:
We recommend the **Vice President, Chief Information Security Officer, Vice President, Network & Compute Technology, and Vice President, Technology Applications,** develop a plan of action and milestones to [redacted] application.

Management Response/Action Plan:
Management agrees with this recommendation. The Vice President Chief Information Security Officer is responsible for managing the completion of remediation through the Assessment & Authorization process (A&A).

The Vice President, Chief Information Security Officer, Vice President, Network & Compute Technology, and Vice President, Technology Applications, will work together to create a plan to [redacted] as defined in the A&A for the [redacted] application.

The A&A process is detail [redacted] in the [redacted] playbook, included with this Management Response.

[redacted]

Target Implementation Date:
March 29, 2024

Responsible Official:
Vice President, Technology Applications and Vice President, Chief Information Security Officer

Recommendation 3:
We recommend the **Vice President, Chief Information Security Officer, Vice President, Network & Compute Technology, and Vice President, Technology Applications,** develop a plan to review medium, low, and informational vulnerabilities that could impact the [redacted] application and remediate these vulnerabilities, as appropriate.

Management Response/Action Plan:

The Vice President, Network & Compute Technology, and Vice President, Technology Applications, will review the reports provided by the Vice President, Chief Information

Security Officer and will prioritize and develop a plan to resolve as appropriate the medium, low, and informational findings for the [redacted] application.

Target Implementation Date:
March 29, 2024

Responsible Official:
Vice President, Technology Applications

Recommendation 4:
We recommend the **Vice President, Technology Applications**, [redacted]

Management Response/Action Plan:
[redacted]

Target Implementation Date:
April 15, 2024

Responsible Official:
Vice President, Technology Applications

E-SIGNED by HEATHER.L DYER
on 2023-12-01 14:11:14 EST

Heather Dyer
Vice President, Chief Information Security Officer

E-SIGNED by WILLIAM.E KOETZ
on 2023-12-01 12:33:49 EST

William E. Koetz
Vice President, Network & Compute Technology

E-SIGNED by ANGELA.D LAWSON
on 2023-12-01 11:26:07 EST

Angela D. Lawson
Vice President, Technology Applications

cc: Corporate Audit Response Management

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