Office of Inspector General | United States Postal Service

Audit Report

Review of the National Change of Address and Moversguide Applications

Report Number 21-146-R22 | September 22, 2022

Table of Contents

Highlights

Background

The U.S. Postal Service processes approximately 98,000 address changes per day. The National Change of Address (NCOA) is the system of record for all change of address requests and stores approximately 160 million change of address records. The Postal Service processed nearly 36 million address changes in 2021, with over 20 million submitted online through the Moversguide application.

What We Did

Our objective was to evaluate the effectiveness of the Postal Service's controls over the security and availability of the NCOA and Moversguide applications. To answer our objective, we performed [redacted] and [redacted] of the applications' [redacted] We also assessed controls over the availability of the applications and their [redacted].

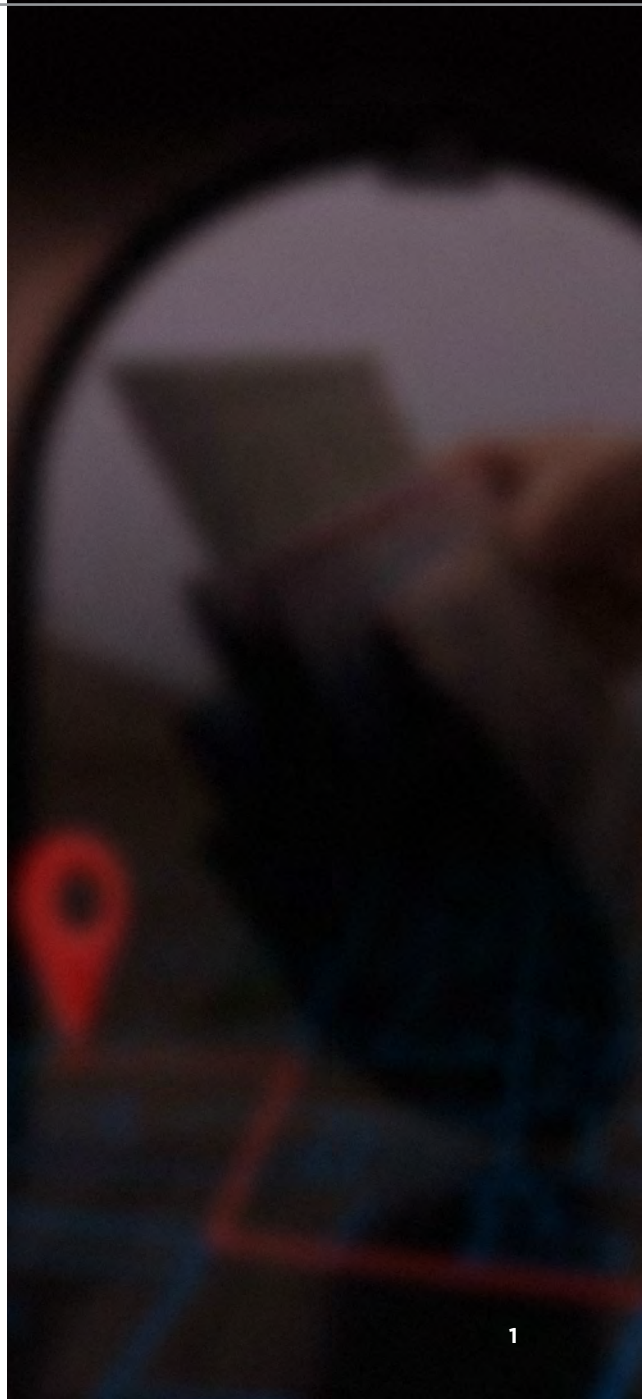
What We Found

The Postal Service's controls over availability of the NCOA and Moversguide applications were generally effective. Specifically, the applications were monitored to ensure they met business availability requirements. However, [redacted] over both applications were not effective. Administrators did not always [redacted]

[redacted] Finally, we found that employees did not [redacted]. This occurred because management did not define roles and responsibilities for [redacted] Additionally, due to potential operational and performance issues the Corporate Information Security Office did not [redacted]. Finally, there was no formal process for [redacted]

Recommendations

We made seven recommendations, [redacted]



Transmittal Letter

OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

September 22, 2022

MEMORANDUM FOR: JEFFREY C. JOHNSON
VICE PRESIDENT, ENTERPRISE ANALYTICS

HEATHER L. DYER
VICE PRESIDENT, CHIEF INFORMATION SECURITY OFFICER

WILLIAM E. KOETZ
VICE PRESIDENT, NETWORK AND COMPUTE TECHNOLOGY

Margaret B. McDavid

FROM: Margaret B. McDavid
Deputy Assistant Inspector General
for Inspection Service and Cybersecurity & Technology

SUBJECT: Audit Report – Review of the National Change of Address and Moversguide Applications (Report Number 21-146-R22)

This report presents the results of our Review of the National Change of Address and Moversguide applications audit.

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

Attachment

cc: Postmaster General
Corporate Audit Response Management

Results

Introduction/Objective

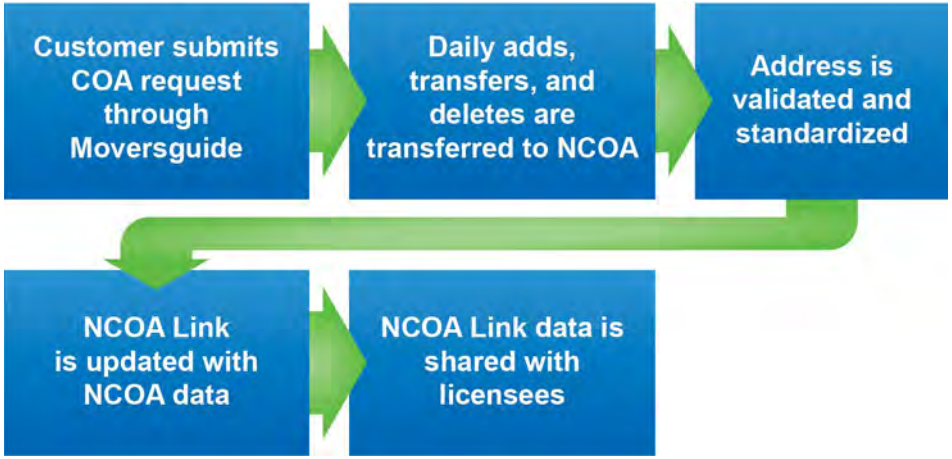
This report presents the results of our self-initiated audit of the National Change of Address and Moversguide Applications (Project Number 21-146). Our objective was to evaluate the effectiveness of the U.S. Postal Service's controls over the security and availability of the National Change of Address (NCOA)[1] and Moversguide applications. See Appendix A for additional information about this audit.

Background

The Postal Service processes approximately 98,000 address changes per day.[2] A change of address (COA) request tells the Postal Service to reroute mail, including letters, packages, and flats,[3] for all or selected individuals at the specified address. Customers can submit COA requests in person, by mail, or online via the Moversguide application. In 2021, the Postal Service processed nearly 36 million COA requests, completing approximately 20 million (56 percent) from applications submitted online.

NCOA is the system of record for all COA requests and is used to produce the NCOA Link product, which is a secure dataset of approximately 160 million permanent COA records. NCOA enables business mailers to process and update mailing lists prior to mailing. The NCOA Link data is provided securely on a regular basis to companies that have purchased the NCOA Link product.[4] See Figure 1 for the Moversguide and NCOA process.

Figure 1. Moversguide and NCOA Online Change of Address Process



Source: U.S. Postal Service Office of Inspector General (OIG) analysis of online change of address process based on the Postal Service COA Controls and Protections dated March 2020.

In recent years, there has been concern over the COA process when executed online due to availability issues and an increase in fraud. The OIG issued a management alert in 2021[5] that identified several social media complaints and reports in national news concerning the availability of the COA systems from August through October 2020. We recommended the Postal Service identify the root cause and remediate the availability issues, which they resolved enabling us to close the recommendations. We also stated our intent to review the COA process to validate that the availability issue was fully resolved.

1 According to the Enterprise Information Repository, NCOA is defined as the database of record for COA requests and an application compromised of several modules. For the purposes of this report, we will refer to it as an application.
2 Postal Facts 2021, Fact #75, updated 4/2/2021.
3 Large envelopes, newsletters, and magazines.
4 NCOA Link | Postal Pro.
5 Management Alert – *Issues Submitting and Processing Change of Address Requests,* 21-017-R21, February 2, 2021.

While conducting this audit, we issued a second management alert in 2022[6] that identified issues with [redacted] in the Moversguide application. We recommended that the Postal Service: 1) develop controls to verify that change of address requests are authorized by the resident of the address and 2) ensure controls are in place to verify the customer's identity when they sign up for [redacted] through the Moversguide application. The Postal Service provided support to close recommendation 2 and plans to resolve recommendation 1 by November 30, 2022.

Findings Summary

We verified that the availability issues identified in the 2021 management alert were resolved and concluded that the Postal Service's controls over availability of the NCOA and Moversguide applications were generally effective. However, we found [redacted] in the NCOA and Moversguide applications. In addition, the Postal Service did not always [redacted] Finally, employees did not follow policies for [redacted]

Finding #1: Application Availability

The Postal Service effectively demonstrated their availability monitoring process, and we did not identify any further issues for the period we reviewed. In addition, the availability issues we reported in the 2021 management alert were resolved. Specifically, the Postal Service fulfilled all transactions that were missed due to the availability issues, provided refunds for the COAs that were not processed, and updated the application to automatically refund customers if a similar issue occurs in the future. Therefore, we concluded that the Postal Service's controls over availability of the NCOA and Moversguide applications were generally effective.

> *"The Postal Service fulfilled all transactions that were missed due to the availability issues, provided refunds for the COAs that were not processed, and updated the application to automatically refund customers if a similar issue occurs in the future."*

Finding #2: [redacted]

System and database administrators [redacted] from the NCOA and Moversguide [redacted]. Specifically, we identified [redacted] in these three parts of the NCOA and Moversguide applications. See Table 1 for summary of key [redacted] found.

Table 1. Summary of NCOA and Moversguide [redacted]

	NCOA	Moversguide
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Source: OIG summary of [redacted]

6 Management Alert – *Issues Identified with Internet Change of Address*, 22-058-R22, April 12, 2022.
7 [redacted]

[redacted]

During our scans of the [redacted], we identified [redacted] for NCOA and [redacted] for Moversguide. [redacted] we identified, [redacted] on the NCOA application and [redacted] on the Moversguide application were associated with the [redacted] During our audit, the Postal Service began implementing the [redacted] The Directive's objective is to reduce the [redacted] Postal Service supports this objective through the [redacted]. For example, they created a [redacted]

[redacted]

Figure 2. [redacted]

[redacted]

Source: OIG analysis of [redacted]

We also found administrators did not [redacted] For example, we found [redacted] Postal Service policy[14] states that only authorized software currently supported and receiving necessary security updates should be installed.

8 [redacted]
9
10
11
12 Handbook AS-805, *Information Security*, Section 9-7.3.4, [redacted] Management Agreement, dated June 2021.
13 [redacted], dated October 2021.
14 Handbook AS-805, Section 10-4.7.3, Vendor Software Support, dated June 2021.

[redacted]

Further, administrators [redacted] the NCOA and Moversguide [redacted] as required by policy. Our review of the [redacted] identified [redacted] for NCOA and [redacted] for Moversguide. For one of these [redacted] related to the Moversguide, we found [redacted] with [redacted] that were not changed. In addition, [redacted] to the Moversguide [redacted] to [redacted]. Postal Service policy requires changing well-known [redacted] for all [redacted].

[redacted]

Finally, administrators [redacted] the Moversguide [redacted]

> "[redacted]. Postal Service

standards[17] require including only features and capabilities needed to ensure the product is secure.

This occurred because management did not [redacted]

Recommendation #1
We recommend the **Vice President, Network and Compute Technology**, develop a formal process and [redacted] for the National Change of Address and Moversguide [redacted].

Recommendation #2
We recommend the **Vice President, Chief Information Security Officer**, develop a continuous process to [redacted].

Recommendation #3
We recommend the **Vice President, Network and Compute Technology**, [redacted] for the National Change of Address and Moversguide [redacted].

Recommendation #4
We recommend the **Vice President, Chief Information Security Officer**, [redacted] for the Moversguide [redacted].

15 [redacted]
16
17 *USPS Coding Secure Software Standards*, Section 3.1.3 Secure by Default, dated 7/15/2019,
18 Established to prevent, respond to, and investigate incidents of cybercrime against the Postal Service.

Finding #3: [redacted] Review

Development teams for the NCOA and Moversguide applications [redacted]

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

> *"We reviewed a [redacted] for the Moversguide [redacted] dated August 26, 2021 and noted [redacted]."*

Additionally, we found that development teams [redacted]. Specifically, we reviewed a [redacted] for the Moversguide application dated August 26, 2021 and noted [redacted]. This occurred because the development teams were not [redacted]

[redacted]

[redacted]

Recommendation #5

We recommend the **Vice President, Enterprise Analytics**, incorporate [redacted]

Recommendation #6

We recommend the **Vice President, Chief Information Security Officer** and **Vice President, Enterprise Analytics**, review the [redacted]

Finding #4: [redacted]

We found that administrators [redacted] for the NCOA and Moversguide applications. [redacted]

19 [redacted]
20 MITRE Corporation, obtained April 5, 2022.
21 [redacted]

Additionally, part of the Moversguide application [redacted]

> "[redacted] for the Moversguide application.

Recommendation #7

We recommend the **Vice President, Chief Information Security Officer** and **Vice President, Enterprise Analytics**, [redacted] for the National Change of Address application as required by policy.

Recommendation #8

We recommend the **Vice President, Chief Information Security Officer**, [redacted] for the National Change of Address application [redacted]

Management's Comments

Management agreed with findings 1, 2, and 3 and disagreed with finding 4. Management agreed with recommendations 1 through 7 and disagreed with recommendation 8. See Appendix B for management's comments in their entirety.

Regarding finding 4, management disagreed that NCOA [redacted]. They stated that the NCOA product is a series of batch jobs, and the [redacted] are maintained in a separate product, and any failures are reported to the NCOA development teams for resolution. Additionally, management stated that these [redacted] are stored in the [redacted]

Regarding recommendation 1, management agreed to develop a formal process that [redacted] on the NCOA and Moversguide [redacted]. The target implementation date is January 31, 2023.

Regarding recommendation 2, management agreed to [redacted] The target implementation date is March 31, 2023.

Regarding recommendation 3, management stated that they provided evidence showing that they have addressed all [redacted] They stated that the [redacted] have updated the quarterly [redacted] process to ensure that the [redacted] from Network and Compute Technology and CISO are incorporated into standard operating procedures. Finally, management stated that the recommendation related to [redacted] should be closed and they [redacted] between March and May 2022. The target implementation date is October 31, 2022.

22 [redacted]
23

Regarding recommendation 4, management agreed to establish timelines for the [redacted] classified as [redacted] based on resource availability and impact to other dependent [redacted]. The target implementation date is January 31, 2023.

Regarding recommendation 5, management stated that they implemented procedures to perform [redacted] to identify [redacted] and requested that this recommendation be closed upon issuance of the report.

Regarding recommendation 6, management stated they have implemented procedures to ensure that [redacted] therefore, management requested closure of the recommendation upon issuance of the report.

Regarding recommendation 7, management stated that they will define standard operating procedures for the [redacted]. They provided support to show that NCOA [redacted] are currently being captured and requested to close this recommendation upon issuance of the report.

Regarding recommendation 8, management disagreed and stated that CISO interpreted the finding to require a [redacted]. They stated that their policy requires the [redacted] teams to perform this function.

Evaluation of Management's Comments

The OIG considers management's comments responsive to recommendations 1-7 and action plans to address these recommendations should resolve the issues identified in the report. We consider management comments nonresponsive to recommendation 8 in the report.

Regarding finding 4, we are aware of the [redacted] that identify transactions between the [redacted], and are reported to the NCOA development team for resolutions. However, the [redacted] Importantly, as noted in response to recommendation 7, NCOA [redacted] are currently being captured and should address our concerns.

Regarding recommendation 3, management provided support to confirm that they [redacted] on the Moversguide [redacted] for [redacted]. However, they did not provide support to show that all the [redacted]. Therefore, we cannot close this recommendation upon issuance of this report and the target implementation date remains October 31, 2022.

Regarding recommendation 5, we verified that management implemented procedures to perform [redacted] and agree to close this recommendation upon issuance of the report.

Regarding recommendation 6, we verified that management reviewed the [redacted]. Additionally, they implemented procedures to ensure [redacted] therefore, we agree to close this recommendation upon issuance of the report.

Regarding recommendation 7, we verified that [redacted] for the NCOA [redacted] are currently being captured and agree to close this recommendation upon issuance of the report.

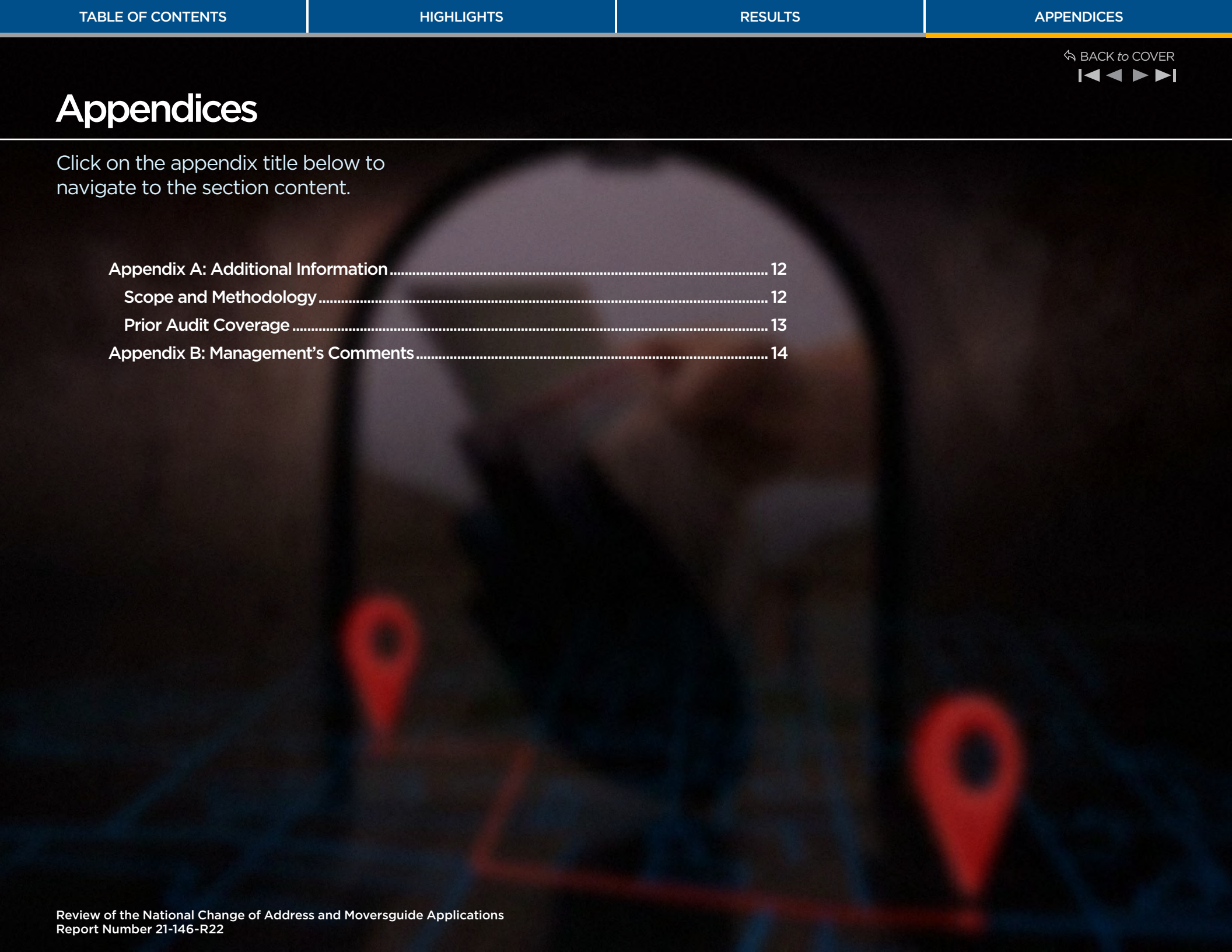
Regarding recommendation 8, we do not state in the recommendation that the [redacted], but only those related the NCOA product. Additionally, policy does not require the [redacted] teams to perform this function. Handbook AS-805 states that [redacted] should be uploaded to a [redacted] and that CISO must have access to all [redacted]. Additionally, Management Instruction AS-800-2022-2 states that all [redacted] must be configured to deliver [redacted] where Cybersecurity Operations Center personnel can analyze them. While we agree that it is not clear in policy whose responsibility it is to forward [redacted], the [redacted] teams do not have this access and therefore cannot perform this function.

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. We consider recommendations 5, 6, and 7 closed with the issuance of this report. We view the disagreement with recommendation 8 as unresolved and plan to pursue it through the audit resolution process.

Appendices

Click on the appendix title below to navigate to the section content.



Appendix A: Additional Information

Scope and Methodology

Our audit scope included assessing controls over the availability of the NCOA and Moversguide applications; and assessing the security of the applications [redacted].

To accomplish our objective, we:

- Obtained and reviewed process flow diagrams and reviewed roles and responsibilities outlined in these processes.
- Gained an understanding of the after-action report generated because of the change implemented to production that caused 1.8 million change of address requests to go unprocessed for three weeks.
- Reviewed change management policies and procedures for testing, approving, and implementing changes to the production environment.
- Reviewed data from monitoring tools to confirm the availability of change of address applications and [redacted] met business requirements.
- Verified whether there are any Service Level Agreements related to the availability of NCOA and Moversguide applications.
- Conducted a [redacted] of NCOA and Moversguide [redacted].
- Conducted a [redacted] of the NCOA and Moversguide applications.
- Interviewed key personnel to gain an understanding of the functions of the change of address systems and [redacted].

We conducted this performance audit from May 2021 through September 2022 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 July 20, 2022 and included their comments where appropriate.

We assessed the reliability of computer-generated data from our automated testing by analyzing and reviewing the raw data, performing automated and manual 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 (in millions)
Issues Identified with Internet Change of Address	Notify Postal Service management of risks associated with ineffective identify verification controls on the Moversguide application.	22-258-R22	4/12/2022	$21.8
Management Alert Issues Submitting and Processing Change of Address Request	Provide Postal Service officials notification of the issues present in the change of address system.	21-017-R21	2/2/2021	None
Change of Address Identity Verification Internal Controls	Evaluate and present results regarding the Postal Service's identity verification internal controls for NCOA service.	MS-AR-18-005	8/24/2018	None

Appendix B: Management's Comments

UNITED STATES POSTAL SERVICE

September 6, 2022

John Cihota,
Director, Audit Services

SUBJECT: **Review of the National Change of Address and Moversguide Applications (21-146)**

Finding #1:

The Postal Service effectively demonstrated their availability monitoring process, and we did not identify any further issues for the period we reviewed. In addition, the availability issues we reported in the 2021 management alert were resolved. Specifically, the Postal Service fulfilled all transactions that were missed due to the availability issues, provided refunds for the COAs that were not processed, and updated the application to automatically refund customers if a similar issue occurs in the future. Therefore, we concluded that the Postal Service's controls over availability of the NCOA and Moversguide applications were generally effective.

Management Response:

Management agrees with the finding.

Finding #2:

[redacted] NCOA and Moversguide [redacted] Specifically, we identified [redacted] in these three parts of the NCOA and Moversguide [redacted]

Management Response:

Management agrees with the finding as it relates to [redacted] and will coordinate between NCT and Enterprise Analytics to [redacted] as appropriate.

Finding #3:

Development teams for the NCOA and Moversguide applications did not follow Postal Service [redacted] During our [redacted] we found:

- [redacted] Postal Service [redacted]

- Incoming Internet requests were not [redacted] Postal Service secure [redacted]
- [redacted] Postal Service [redacted]

Management Response:

Management agrees with the finding.

Finding #4:

We found that administrator [redacted] for the NCOA and Moversguide [redacted] Specifically, they [redacted] Postal Service policy requires [redacted]

Additionally, part of the Moversguide [redacted] Postal Service policy states [redacted] During the audit, Postal Service started [redacted] for the Moversguide [redacted]

This occurred because CISO did not have a formal process that ensures [redacted]

Management Response:

Management disagrees that NCOA [redacted] The NCOA product is primarily a series o [redacted] to the NCOA development teams for resolution. NCOA [redacted]

Recommendation #1:

We recommend the Vice President, Network Compute and Technology, develop a formal process and define responsibility for [redacted] for the National Change of Address and Moversguide [redacted]

Management Response/Action Plan:

Enterprise Analytics will coordinate with Network Compute Technology to develop a formal process that defines the responsibility of each functional area for the update of [redacted] to the National Change of Address and MoversGuide programs.

Target Implementation Date:

1/31/2023

Responsible Official:

Vice President, Enterprise Analytics

Recommendation #2:

We recommend the Vice President, Chief Information Security Officer, develop a continuous process to [redacted]

Management Response/Action Plan:

Management agrees with the recommendation and will develop a plan of action to [redacted]

Target Implementation Date:

3/31/2023

Responsible Official:

Vice President, Chief Information Security Officer

Recommendation #3:

We recommend the Vice President, Network Compute and Technology, [redacted] for the National Change of Address and Moversguide [redacted]

Management Response/Action Plan:

Enterprise Analytics is responsible for the management and oversight of Moversguide and National Change of Address [redacted] Enterprise Analytics works closely with the CISO organization [redacted] Management agrees that we will continue to work closely with the CISO organization as new [redacted] Additionally, the [redacted] have updated the [redacted] Refer to **Mngt Response.zip** for evidence of change. As it relates to [redacted] Management believes we have demonstrated that this item should be closed. NCT works closely with Enterprise Analytics and has [redacted]

Target Implementation Date:

10/31/2022

Responsible Official:

Vice President, Enterprise Analytics

Vice President, Network Compute and Technology

Recommendation #4:

We recommend the Vice President, Chief Information Security Officer, [redacted] for the Moversguide [redacted]

Management Response/Action Plan:

Management agrees with the recommendation. Enterprise Analytics will coordinate with Corporate Information Systems Office to establish [redacted]

Target Implementation Date:

1/31/2023

Responsible Official:

Vice President, Enterprise Analytics

Recommendation #5:

We recommend the Vice President, Enterprise Analytics, incorporate [redacted]

Management Response/Action Plan:

Management agrees with this recommendation. Enterprise Analytics has implemented procedures to [redacted] Refer to **Mngt Response.zip** for evidence of change. Management requests that this recommendation be closed.

Target Implementation Date:

10/31/2022

Responsible Official:

Vice President, Enterprise Analytics

Recommendation #6:

We recommend the Vice President, Chief Information Security Officer and Vice President, Enterprise Analytics, review the [redacted]

Management Response/Action Plan:

Management agrees with this recommendation. Enterprise Analytics has implemented procedures to ensure [redacted] Management requests that this recommendation be closed. Refer to **Mngt Response.zip** for evidence of change.

Target Implementation Date:

10/31/2022

Responsible Official:

Vice President, Enterprise Analytics

Vice President, Chief Information Security Officer

Recommendation #7:

We recommend the Vice President, Chief Information Security Officer and Vice President, Enterprise Analytics, obtain and review [redacted] for the National Change of Address and [redacted] as required by policy.

Management Response/Action Plan:

Management agrees with this recommendation for the review of [redacted] Enterprise Analytics management will define standard operating procedures for the [redacted] Refer to **Mngt Response.zip** for evidence that NCOA [redacted] are currently being captured.

Target Implementation Date:

10/31/2022

Responsible Official:

Vice President, Enterprise Analytics

Recommendation #8:

We recommend the Vice President, Chief Information Security Officer, [redacted] for the National Change of Address [redacted] as required by policy.

Management Response/Action Plan:

Management disagrees with this recommendation. CISO interpreted this finding to require a [redacted] The AS-805 requires the [redacted] teams to perform this function, not a centrally managed function within CISO.

Target Implementation Date:

N/A

Responsible Official:

Vice President, Chief Information Security Officer

E-SIGNED by Jeffrey.C Johnson
on 2022-09-06 12:55:45 CDT

Jeffrey C. Johnson
Vice President, Enterprise Analytics

E-SIGNED by Heather.L Dyer
on 2022-09-06 12:24:36 CDT

Heather L. Dyer
Vice President, Chief Information Security Officer

E-SIGNED by William.E Koetz
on 2022-09-06 12:12:42 CDT

William E. Koetz
Vice President, Network and Compute Technology

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

For media inquiries, please email
press@uspsoig.gov or call 703-248-2100