



OFFICE OF INSPECTOR GENERAL

UNITED STATES POSTAL SERVICE

Address Management Licensing Agreements

Audit Report

Report Number
SM-AR-16-004

December 29, 2015





OFFICE OF INSPECTOR GENERAL

UNITED STATES POSTAL SERVICE

Highlights

The Postal Service did not adequately monitor licensee compliance with five of the six address management licensing products reviewed.

Background

The U.S. Postal Service's Office of Address Management provides value-added products and services that enable business customers to better manage the quality of their mailing lists while maximizing the Postal Service's ability to deliver mail as addressed.

The Office of Address Management's seven address management products generated revenue totaling \$14.3 million in fiscal year 2015. We evaluated six of the seven products. (The seventh product was recently reviewed in a separate audit.) For these products, the Postal Service executed 421 licenses to customers.

Customers that license address management products containing sensitive or critical data are subject to site security reviews to evaluate the physical security of the data. These reviews evaluate physical security controls to protect Postal Service information such as facilities, personnel, hardware, and software. According to Postal Service policy, site security reviews must be conducted at least every 3 years but can be conducted at any time.

Our objectives were to determine whether the Postal Service monitors licensee compliance with address management licensing agreements and evaluate whether these agreements adequately protect the Postal Service's interests.

What The OIG Found

The Postal Service did not adequately monitor licensee compliance with five of the six address management licensing products reviewed. Additionally, although licensing agreements protected the Postal Service's intellectual property and ability to take legal action, it could improve the language of the agreement template to better protect its interests. The Postal Service did not conduct site security reviews at any of the licensees' locations for the five products that required them.

Management considered the reviews unnecessary because Postal Service data were encrypted; however, encryption does not eliminate all security risks. Inadequate physical security controls could affect the confidentiality, integrity, and availability of Postal Service assets and increase the risk of unauthorized use of address management information.

Also, the licensing agreement templates for all six address management products needed updating to ensure the agreements were accurate and protected the Postal Service's interests. The templates contained outdated or inconsistent provisions, such as references to old policies and governing law. The Postal Service did not periodically evaluate and update licensing agreement language and only updated the templates to reflect price changes.



OFFICE OF INSPECTOR GENERAL

UNITED STATES POSTAL SERVICE

Without updated and consistent provisions, there is an increased risk that licensees may misinterpret requirements, resulting in unnecessary expenditures of time and money if the Postal Service needs to enforce provisions within the agreements. The Postal Service was unable to provide us any documentation to support that it had ever enforced an agreement.

Finally, during our fieldwork, we identified issues with the maintenance of credit card payment data for address management products. We addressed these concerns in a separate management alert.

What The OIG Recommended

We recommended that management conduct required site security reviews of address management licensees; and periodically evaluate licensing agreement templates to determine if provisions are up-to-date, include consistent language, and adequately protect Postal Service interests.

Transmittal Letter



OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

December 29, 2015

MEMORANDUM FOR: ROBERT CINTRON
VICE PRESIDENT, ENTERPRISE ANALYTICS

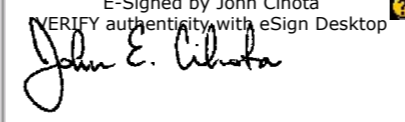
JAMES D. WILSON
MANAGER, ADDRESS MANAGEMENT

LYNNE M. MITCHELL
ACTING MANAGER, CORPORATE
INFORMATION SECURITY

DAVID G. BOWERS
POSTAL INSPECTOR IN CHARGE, SECURITY AND
CRIME PREVENTION

KEVIN A. CALAMONERI
DEPUTY GENERAL COUNSEL

E-Signed by John Cihota
VERIFY authenticity with eSign Desktop



FROM: John E. Cihota
Deputy Assistant Inspector General
for Finance and Supply Management

SUBJECT: Audit Report – Address Management Licensing Agreements
(Report Number SM-AR-16-004)

This report presents the results of our audit of the U.S. Postal Service's Address Management Licensing Agreements (Project Number 15BG004SM000).

We appreciate the cooperation and courtesies provided by your staff. If you have any questions or need additional information, please contact Keshia L. Trafton, director, Supply Management and Facilities, or me at 703-248-2100.

Attachment

cc: Corporate Audit and Response Management

Table of Contents

Cover	
Highlights.....	1
Background.....	1
What The OIG Found.....	1
What The OIG Recommended	2
Transmittal Letter.....	3
Findings.....	5
Introduction	5
Summary.....	6
Monitoring Licensee Compliance.....	6
Licensing Agreements.....	7
Recommendations.....	9
Management’s Comments	9
Evaluation of Management’s Comments	10
Appendices.....	11
Appendix A: Additional Information	12
Background	12
Objectives, Scope, and Methodology.....	13
Prior Audit Coverage	14
Appendix B: Management’s Comments.....	15
Contact Information	18

Findings

The Office of Address Management's seven address management products generated revenue totaling \$14.3 million in FY 2015. We evaluated six of these seven products. For these six products, the Postal Service executed 421 licenses to customers.

Introduction

This report presents the results of our self-initiated audit of the U.S. Postal Service's Address Management Licensing Agreements¹ (Project Number 15BG004SM000). Our objectives were to determine whether the Postal Service monitors licensee compliance with address management licensing agreements and evaluate whether the licensing agreements adequately protect the Postal Service's interests. See [Appendix A](#) for additional information about this audit and a description of the address management products we reviewed.

The Postal Service's Office of Address Management is located at the National Customer Support Center (NCSC) in Memphis, TN. The office provides value-added products and services that enable business customers to better manage the quality of their mailing lists while maximizing the Postal Service's ability to efficiently deliver mail as addressed.

The Office of Address Management's seven address management products generated revenue totaling \$14.3 million in fiscal year (FY) 2015. We evaluated six of these seven products.² For these six products, the Postal Service executed 421³ licenses to customers.

We reviewed 140 of the 421 licensing agreements and all nine standard templates for the following six address management products (see Table 1).

Table 1. Address Management Licensing Agreements Reviewed

Total	421 Total Agreements
	140 OIG Reviewed ⁴

Source: Postal Service NCSC data as of January 9, 2015.

- 1 A contract under which the licensor for an agreed-upon consideration grants to the licensee certain rights with respect to intellectual property (for example, trademarks, patents, or copyrights) of the licensor.
- 2 The U.S. Postal Service Office of Inspector General (OIG) issued a report on the *National Change of Address Program* (Report Number [IT-AR-14-010](#), dated September 24, 2014). As a result, the NCOA product is not included in the scope of this audit.
- 3 The number of licenses for the six address management products we reviewed as of January 9, 2015.
- 4 The OIG judgmentally selected and reviewed a sample of 140 of the 421 executed address management licensing agreements for the six address management products.

Without updated and consistent provisions, there is an increased risk that licensees could misinterpret requirements, resulting in unnecessary expenditures of time and money if the Postal Service needs to enforce provisions of the agreements. The Postal Service was unable to provide us with any documentation to support that it has ever enforced an agreement.

Address management product licensees must comply with licensing agreement provisions for securing Postal Service data by, among other things, maintaining a secure environment over hardware and software and restricting unauthorized access to Postal Service data. For some of these products, the Postal Service is required to conduct a site security review to evaluate the physical security of Postal Service information.⁵ We evaluated whether or not the Postal Service monitored licensee compliance with licensing agreements and conducted site security reviews, as required.

During our fieldwork at the NCSC, we identified security issues with the maintenance of credit card payment data for address management products. The OIG issued a management alert titled *Controls Over Credit Card Data at the National Customer Support Center* to address these concerns.⁶

Summary

The Postal Service did not adequately monitor licensee compliance with five of the six address management products reviewed. Additionally, although agreements protected the Postal Service's intellectual property and ability to take legal action, it could improve the language of the agreement template to better protect its interests.

Specifically, the Postal Service did not conduct site security reviews at any licensee locations for the five products that required them. Management considered the reviews unnecessary because the Postal Service's data were encrypted; however, encryption does not eliminate all security risks. Inadequate physical security controls could affect the confidentiality, integrity, and availability of Postal Service assets and increase the risk of unauthorized use of address management information.

In addition, the licensing agreement templates for all six address management products we reviewed needed updating to ensure the agreements were accurate and protected the Postal Service's interests. The templates contained outdated or inconsistent provisions, such as references to old policies and governing law. The Postal Service did not periodically evaluate and update licensing agreement language; rather, it only updated the templates to reflect price changes.

Without updated and consistent provisions, there is an increased risk that licensees could misinterpret requirements, resulting in unnecessary expenditures of time and money if the Postal Service needs to enforce provisions of the agreements. The Postal Service was unable to provide us with any documentation to support that it has ever enforced an agreement. Additionally, the Postal Service cannot ensure all agreements are in its best interest, and it may lose the benefit of recently identified best practices when it does not update language.

Finally, during our fieldwork, we identified issues with the maintenance of credit card payment data for address management products. We addressed these concerns in a separate management alert.

Monitoring Licensee Compliance

The Postal Service did not conduct site security reviews to monitor compliance for the five address management products that required them.⁷ Specifically, the Postal Service did not review whether licensees complied with physical security controls over

⁵ Site security reviews evaluate risks as they relate to the physical security of applications and the information resources hosting them. They include security evaluations of locations, facilities, personnel, controlled areas, environments, communications, hardware, software, information, administrative, emergency response and contingency planning, as well as auditing and monitoring. According to Postal Service policy, these reviews must be conducted at least every 3 years but can be conducted at any time.

⁶ Report Number [SM-MA-15-003](#), dated September 11, 2015.

⁷ AMS API does not require site security reviews to use this product because it is not sensitive-enhanced or critical.

Postal Service policy requires all business partners housing sensitive-enhanced information resources to have a site security review, regardless of their location. Additionally, address management licensing templates for four products state the licensee agrees to provide security for all licensed materials that is equal to or greater than the level of security necessary for compliance.

Postal Service applications and information resources⁸, as required.⁹ Physical security includes protection of items such as facilities, personnel, hardware, and software.¹⁰

Prior to August 2001, the Postal Service maintained unencrypted address management data which licensees could copy. It was during this time (the 1990s) the Postal Service stated that it had a more robust audit function and conducted site security reviews; however, we were unable to verify whether these reviews occurred. In August 2001, the Office of Address Management encrypted address data. Management stated that this control adequately secured data and prevented unauthorized use, such as creating unauthorized mailing lists. Management further stated they were confident licensees were complying with their agreements but could not provide evidence to support this claim. While encryption provides additional security for data, site security reviews of the physical environment fully assess the overall security environment.

Postal Service policy requires all business partners housing sensitive-enhanced information resources¹¹ to have a site security review, regardless of their location.¹² Additionally, address management licensing templates for four products¹³ state the licensee agrees to provide security for all licensed materials that is equal to or greater than the level of security necessary for compliance.¹⁴ The handbook establishes information security policies to appropriately identify, classify, and protect information resources from accidental or intentional unauthorized use, modification, disclosure, or destruction. Site security reviews would help the Postal Service verify that licensees are complying with licensing agreements. Inadequate physical security controls could affect the confidentiality of Postal Service information resources and increase the risk of unauthorized use of the Postal Service's address management information.

Licensing Agreements

We sampled 140 of the 421 executed address management licensing agreements and determined the licensee agreements were consistent with agreement templates and signed by authorized Postal Service personnel. In addition, the licensing agreements protected the Postal Service's intellectual property and ability to take legal action. However, the Postal Service could improve licensing agreement template language for all six address management products to better protect its interests. For example, licensees may misinterpret inconsistent or outdated provisions resulting in unnecessary expenditures of time and money if the Postal Service attempts to enforce agreements. The Postal Service was unable to provide us with any documentation to support that it had ever enforced an agreement. The Postal Service should be consistent across all licensing agreements unless there is a business reason not to be. We noted that the following template provisions were inconsistent or outdated:

- **Governing law.** The Postal Service was not consistent with what law applied to the agreement and where lawsuits should be litigated. Specifically, licensing agreement templates governed by federal law stated that the venue for litigation, "if possible," was the District of Columbia; however, three agreements stated that when federal laws are not applicable and no lawsuit venue is chosen, the Postal Service should defer to New York state law instead of District of Columbia law.¹⁵

⁸ Information resources are strategic assets vital to the business performance of the Postal Service. Examples of information resources include Postal Service operating systems, databases, and programs.

⁹ Handbook AS-805-A, *Information Resource Certification and Accreditation Process*, Sections 4-3.4.7 and 4-3.4.7.1, June 2015.

¹⁰ Handbook AS-805-A, Section 4-3.4.7.1.

¹¹ Information related to the protection of Postal Service restricted financial information, trade secrets, proprietary information, and emergency preparedness.

¹² Handbook AS-805, Section 4-1.

¹³ The four address management licensing templates are DSF², DPV, LACSLink, and SuiteLink. The RDI template does not specifically state that licensees are required to comply with Handbook AS-805 within the agreement; however, it is a sensitive-enhanced product and must have site security reviews in accordance with Handbook AS-805.

¹⁴ Licensing agreements inform licensees that Handbook AS-805, *Information Security*, is available on the Postal Service's website.

¹⁵ DSF², DPV, and RDI licensing agreements were governed by New York state law when federal laws were not applicable, as interpreted by the U.S. Court of Appeals for the Second Circuit.

- Termination due to asset transfer. Each licensing agreement template specified the agreement would be terminated if assets were transferred to a new entity due to a merger or acquisition; however, Suite^{Link}® stated an ownership transfer of 30 percent of assets would initiate termination. This is inconsistent with other agreements that did not establish a threshold for asset transfer prior to agreement termination.
- Policy references. Five licensing agreement templates referenced the *Purchasing Manual* as the current Postal Service contracting policy. However, in 2005, *Supplying Principles & Practices*¹⁶ replaced the *Purchasing Manual*; therefore, this language is outdated.
- Termination notices. The AMS API licensing agreement template had a termination notice provision requiring the Postal Service to give licensees a 1-year notice for cancellation. This was inconsistent with the other agreement templates which had shorter terms.
- Dispute resolution requirements. The AMS API licensing agreement template required arbitration prior to litigation. This was inconsistent with the other agreement templates that did not require arbitration prior to litigation.

The outdated language and inconsistencies in licensing agreement templates occurred because the Postal Service did not periodically evaluate and update them. Management stated they only update agreement templates when prices change.

The Postal Service should be consistent in its approach across all agreements unless there is a business reason not to be. For example, the DPV licensing template states that if no federal law applies, the agreement is governed by the laws of the state of New York. However, the LACS^{Link}® Developer Agreement is governed only by federal law and does not refer to the laws of New York. If one of the jurisdictions is generally beneficial for the Postal Service, then both agreements should be governed by that law. Additionally, the Postal Service cannot ensure all agreements are in its best interests and it may lose the benefit of recently identified best practices when it uses inconsistent language without a valid business reason.

¹⁶ A set of business principles and accompanying business practices that provide guidance to Postal Service supply chain management employees engaged in purchasing and supplying activities.

Recommendations

We recommend the vice president, Enterprise Analytics, direct the manager, Address Management, to coordinate with the acting manager, Corporate Information Security, and postal inspector in charge, Security and Crime Prevention, to:

1. Implement a process and plan of action to conduct required site security reviews of address management licensees to verify adherence with license agreements.

We recommend the vice president, Enterprise Analytics, direct the manager, Address Management, to coordinate with the deputy general counsel, to:

2. Periodically evaluate licensing agreement templates to determine whether provisions are consistent, up-to-date, and adequately protect the Postal Service's best interests.

Management's Comments

Management agreed with one finding but disagreed with the finding pertaining to the need for physical site security reviews. Management agreed with both recommendations.

Management stated that Address Management plays a critical role in maintaining and disseminating address information required by the mailing industry to generate addresses that are complete, correct, and current. Additionally, the mailing industry depends upon the availability of address management products in formats that are easy to obtain and use. Management further stated that Address Management has created technology to secure the information contained in these products in a manner that satisfies both customer expectations and its legal responsibilities. They also stated that users are only able to access information in address management products through defined procedures, and a user cannot manipulate or circumvent the procedures to gain access to unauthorized information.

Management disagreed that physical site security reviews were needed for all address management products. Management believes the security embodied within these products sufficiently protects the confidentiality, integrity, and availability of these assets and minimizes the risks of unauthorized use of address management information. However, management agreed to review the security policies in Handbook AS-805-A as it relates to address management products and establish a process for site security reviews, if necessary.

Regarding recommendation 1, management stated they will review Postal Service policies and the sensitivity classification of all address management products. Management further stated they will update address management licenses to reflect the classification of sensitivity for each product based on the results of these reviews and in conjunction with actions that may be taken in response to recommendation 2. Management further stated the performance of onsite security reviews for products will be based on the value added as determined by the business owner. Procedures will be implemented for site security reviews to ensure licensee adherence to license agreement terms and conditions. The target implementation date is January 1, 2017.

Regarding recommendation 2, management stated a plan will be implemented to update three licenses by January 31, 2017, and the remaining three by January 31, 2018. Thereafter, management stated address management product licenses will be reviewed approximately once every 3 years, unless circumstances warrant an earlier review. The target implementation date is January 31, 2018.

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

Evaluation of Management's Comments

The OIG considers management's comments responsive to the recommendations in the report.

Regarding management's disagreement with the need for physical site security reviews, we believe inadequate physical security controls could affect the confidentiality of Postal Service information resources and increase the risk of unauthorized use of the Postal Service's address management information, as noted in our report. Further, performance of site security reviews would help the Postal Service verify licensee compliance. Notwithstanding, management's planned action to review the security policies and sensitivity classification of address management products and conduct site security reviews based on these results should mitigate the risk of unauthorized use.

All recommendations require OIG concurrence before closure. Consequently, the OIG requests written confirmation when corrective actions are completed. These recommendations should not be closed in the Postal Service's follow-up tracking system until the OIG provides written confirmation that the recommendations can be closed.

Appendices

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

Appendix A: Additional Information	12
Background	12
Objectives, Scope, and Methodology	13
Prior Audit Coverage	14
Appendix B: Management’s Comments.....	15

Appendix A: Additional Information

Background

The Postal Service's Office of Address Management is located at the NCSC in Memphis. This office provides value-added products and services enabling business customers to better manage the quality of their mailing lists while maximizing the Postal Service's ability to efficiently deliver mail as addressed. The seven address management products available to customers produced revenue totaling \$14.3 million during FY 2015. This report reviews six of these products. Because the OIG issued a prior report on the seventh product,¹⁷ we are not including it in the scope of this audit.

The Postal Service treats address management products maintained at the NCSC as confidential and proprietary systems. As a result, address management licensing agreements should adequately protect the Postal Service's interests. We reviewed licensing agreements pertaining to the address management products shown in Table 2.

Table 2. Descriptions of Address Management Products Reviewed

Product	Description
AMS API	AMS API is used to develop address matching software. It may be integrated with a manufacturer's product and redistributed by the manufacturer.
DSF ²	The DSF ² file system helps mailers obtain accurate delivery address information and facilitates identification of erroneous addresses contained in mailers' address files. The DSF ² product also provides additional information such as type of delivery and LACS ^{Link} information. This product helps reduce the amount of Undeliverable as Addressed (UAA) pieces, which, in turn, makes mail processing and delivery operations more efficient.
DPV	The DPV system helps mailers obtain accurate delivery address information and facilitates identification of erroneous addresses in mailer address files. Mailer use of DPV reduces the amount of UAA pieces, which, in turn, makes mail processing and delivery operations more efficient.
LACS ^{Link}	The LACS ^{Link} product is a secure data set of converted addresses that primarily arose from implementation of the 911 system, which commonly involves changing rural-style addresses to city-style addresses. The LACS ^{Link} product also contains existing city-style addresses that have been renamed or renumbered.
RDI [™]	RDI is a data product that helps customers reduce shipping costs by verifying whether a delivery type is classified as residential or business. Since some shipping companies charge a higher price for residential delivery, the RDI product allows customers to make informed shipping decisions.
Suite ^{Link} [®]	The Suite ^{Link} product improves business delivery addresses for multi-occupation buildings, such as high rises, by providing a suite number or other secondary information about an address in response to a customer's inquiry of the Suite ^{Link} product.

Source: The Postal Service NCSC.

¹⁷ *National Change of Address Program* (Report Number [IT-AR-14-010](#), dated September 24, 2014).

Objectives, Scope, and Methodology

Our objectives were to determine whether the Postal Service monitors licensee compliance with address management licensing agreements and evaluate whether the licensing agreements adequately protect the Postal Service's interests. To accomplish our objectives, we:

- Identified six address management products business customers use to better manage the quality of their mailing lists. The scope of this audit did not include the NCOA product because it was included in a prior OIG audit.
- Judgmentally selected and reviewed a sample of 140 of the 421 executed address management licensing agreements for the six address management products.¹⁸
- Evaluated the consistency of licensing agreements to determine whether they adequately protected Postal Service interests and whether the contracting officer or contracting officer representative was authorized to sign the agreements.
- Reviewed all nine address management licensing agreement templates for the six products for consistency and evaluated whether the agreements adequately protected Postal Service interests.
- Completed fieldwork at the NCSC in Memphis.
- Interviewed Postal Service officials from the NCSC and the Postal Service law department.

We conducted this performance audit from October 2014 through December 2015, 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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. We discussed our observations and conclusions with management on November 12, 2015, and included their comments where appropriate.

We did not assess the reliability of any computer-generated data for the purposes of this report. We relied on address management licensing agreement criteria and documentation available on the Postal Service's intranet and licensing agreements provided by the Postal Service for our sample to complete our fieldwork.

¹⁸ Universe as of January 9, 2015.

Prior Audit Coverage

Report Title	Report Number	Final Report Date	Monetary Impact
<i>Controls Over Credit Card Data at the National Customer Support Center</i>	SM-MA-15-003	9/11/2015	None
<p>Report Results: The Postal Service needs to improve controls over credit card data at the NCSC. The NCSC did not follow payment card industry requirements and Postal Service policy for securing credit card information. Specifically, credit card numbers on payment records were not masked; the facility did not require individuals entering the accounting room (where credit card payment information is received) to have identification access badges; and management did not protect video cameras surveilling the accounting room from possible tampering. Without proper controls, the Postal Service is at risk of unauthorized use of credit card numbers. In response to our audit, management now masks credit card numbers stored in the accounting room; will replace combination locks with employee identification access badge readers for the accounting and storage room doors; and has restricted personnel with access to the accounting room from being able to access the storage room.</p>			
<i>National Change of Address Program</i>	IT-AR-14-010	9/24/2014	None
<p>Report Results: NCOA license agreements did not always have sufficient contract provisions to protect customer data and management did not always monitor these agreements for licensee compliance. As a result, there is a risk that unauthorized users could access change of address (COA) data and NCOA data could be breached. The OIG recommended management centralize user account management in eAccess for the COA Forms Processing System, store hard copy COA orders in accordance with policy, re-initiate the NCOA certification and accreditation process, upgrade security software, identify all cooperative database mailers and their activities, and implement a process to ensure current Postal Service requirements are in all license agreements to protect customer information. Finally, we recommended management implement a plan of action for conducting random site security reviews of licensees and evaluate solutions and benefits of automating the acknowledgment forms process. Management agreed with four of the nine recommendations. They agreed to re-initiate the NCOA certification and accreditation process, the security software upgrade, the random site security reviews, and the automation of acknowledgment forms process.</p>			
<i>Delegations of Contracting Authority Outside of Supply Management</i>	SM-AR-14-007	8/5/2014	None
<p>Report Results: Address management officials did not delegate authority for personnel to sign agreements with service providers who provide address quality data correction service to mailers. Without delegating contracting authority, the agreements are not legally binding unless ratified by a Postal Service official with contracting authority. The OIG recommended the postmaster general rescind the delegation to Facilities for real estate service contracts to ensure personnel responsible for signing agreements with the service providers have contracting authority, establish a process for the submission of Facilities' annual financial report of real estate transactions, determine whether Address Quality Service agreements should be ratified, delegate contracting authority to personnel responsible for signing Address Quality Service agreements, and develop a process to identify contracts and agreements that may not have delegations of authority. Management agreed with four of the five recommendations and disagreed with the recommendation to rescind real estate service contract delegation to Facilities.</p>			

Appendix B: Management's Comments



December 15, 2015

LORI LAU DILLARD
DIRECTOR, AUDIT OPERATIONS

SUBJECT: Address Management Licensing Agreements
(Report Number SM-AR-16-DRAFT)

Thank you for the opportunity to review and comment on the subject draft audit report. Management understands the intent of the draft report to help improve the overall posture and capabilities of the Postal Service to defeat and otherwise mitigate cybersecurity risks. Protecting the privacy of customer, employee, supplier and the Postal Service information has been and always will be a priority for the Postal Service. USPS has developed and is executing an aggressive multi-phased cybersecurity improvement strategy to meet its security objectives and to further protect information and assets across the enterprise.

Address Management plays a critical role in maintaining and disseminating address information required by the mailing industry to generate addresses that are complete, correct, and current. The mailing industry depends upon the availability of address management products in formats that are easy to obtain and use. Consistent with our legal responsibilities as defined in 39 U.S.C. § 412 and the Privacy Act, Address Management has created cutting-edge technology to secure the information contained in address management products in a manner that satisfies both the customer expectations and our legal responsibilities. Users are only able to access information in address management products through expressly defined procedures and a user cannot manipulate or circumvent these procedures to gain access to information they are not authorized to receive.

Management agrees with the OIG's finding that address management licensing agreements could be improved with revisions to update the language and make the license agreements more consistent, a process it has already begun. Management disagrees with the OIG's finding regarding the need for physical site security reviews of all the address management products listed. Management does believe that the security embodied within the various address management products sufficiently protects the confidentiality, integrity, and availability of these assets and minimizes the risks of unauthorized use of address management information. Management agrees to conduct a review of our security policies defined in Handbook AS-805-A *Information Resource Certification and Accreditation Process* as it

relates to address management products and, if necessary, establish a process for performing site security reviews.

Management submits the below responses and action plans to the OIG recommendations.

Recommendation 1:

Implement a process and plan of action to conduct required site security reviews of address management licensees to verify adherence to license agreements.

Management Response/Action Plan:

Management agrees with the recommendation. The Manager, Address Management will coordinate with the acting Manager, Corporate Information Security, and the Postal Inspector in Charge, Security and Crime Prevention offices to review Postal Service policies and the sensitivity classifications of all address management products. Based on the determinations of these reviews, and in conjunction with the actions that may be taken in response to Recommendation 2, address management licenses will be updated to reflect the status of the classifications of sensitivity for each product. Performing an onsite security review for products will be based on the amount of value it would add, determined by the business owner. Procedures will be implemented to perform site security reviews to ensure licensee adherence to the terms and conditions contained within the license agreements.

Target Implementation Date:

January 1, 2017

Responsible Official:

Manager, Address Management

Recommendation 2:

Periodically evaluate licensing agreement templates to determine whether provisions are consistent, up-to-date, and adequately protect the Postal Service's best interests.

Management Response/Action Plan:

Management agrees with the recommendation. The Manager, Address Management will coordinate with Deputy General Counsel to evaluate and update license agreements for address management products. A plan will be

implemented to complete the update of 3 licenses by the end of January 2017 and the remaining 3 licenses updated by the end of January 2018. Thereafter, a review of all address management product licenses will be performed approximately once every three years, unless circumstances warrant an earlier review, and results of the review will be documented.

Target Implementation Date:

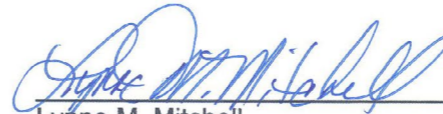
January 31, 2018

Responsible Official:


Manager, Address Management



Robert Cintron
Vice President, Enterprise Analytics



Lynne M. Mitchell
A/Manager, Corporate Information Security



David G. Bowers
Postal Inspector In Charge, Security and Crime Prevention



Kevin A. Calamoneri
Deputy General Counsel

cc: *Manager, Address Management*
Manager, Corporate Audit Response Management



OFFICE OF
**INSPECTOR
GENERAL**
UNITED STATES POSTAL SERVICE

Contact us via our [Hotline](#) and [FOIA](#) forms, follow us on social networks, or call our Hotline at 1-888-877-7644 to report fraud, waste or abuse. Stay informed.

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