OFFICE OF
INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

End User Data Loss Prevention

Audit Report

Report Number
IT-AR-15-005

April 17, 2015

Highlights
Table of Contents
Findings
Recommendations
Appendices

OFFICE OF
INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

Highlights

The Postal Service is at risk of internal users compromising sensitive employee, customer, and business information.

Background

Loss of organizational information by internal users can cause significant financial loss and damage an organization's reputation. Data loss prevention (DLP) systems help prevent internal users from maliciously or unintentionally leaking sensitive information that is personally identifiable, financial, proprietary, or business sensitive. The increasing use of personal computers and mobile devices requires agencies to develop new technologies, such as mobile device management software, to secure corporate data and minimize its loss through [redacted].

The objective of this audit was to determine whether the U.S. Postal Service's DLP and mobile device management systems are operating effectively to prevent internal users from losing data.

What The OIG Found

We determined the DLP and mobile device management systems do not operate effectively to prevent internal users from sending sensitive information outside the Postal Service network. Sensitive information includes personally identifiable, financial or proprietary information, and other business-sensitive data. Although the DLP system does block some emails based on established rules, it [redacted] sensitive information. Current mobile device management security policy does not prevent internal users from accessing [redacted] using Postal Service mobile devices. This lack of controls exists because the Postal Service has not implemented a solution to [redacted]. In addition, business groups are not aware of all DLP services designed to identify sensitive information in documents. In addition, management has not established formal procedures to ensure continuous quality assurance testing of DLP rules or implemented mobile security controls.

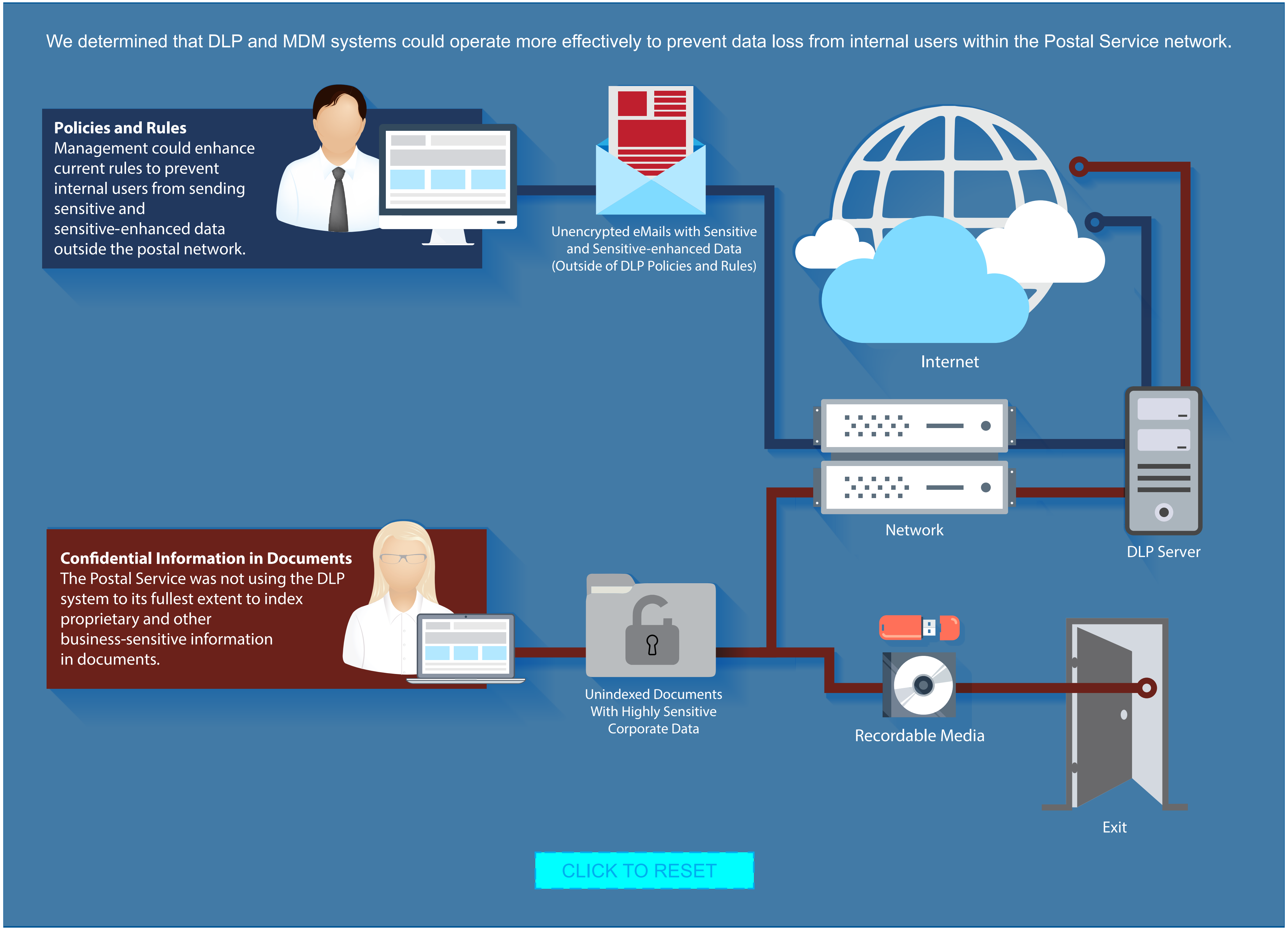
As a result, the Postal Service is at risk of internal users compromising sensitive employee, customer, and business information, which could lead to financial and legal consequences.

What The OIG Recommended

We recommended management implement procedures to require continuous quality assurance tests and reviews to update DLP policies and rules, and a solution to allow the DLP system to [redacted] containing sensitive information. We also recommended management implement DLP procedures and communicate them to employees; and implement a mobile technology solution that [redacted].

Data Loss Prevention and Mobile Device Management Systems Controls

Data loss prevention (DLP) systems help prevent internal users from maliciously or unintentionally leaking sensitive information that is personally identifiable, financial, or proprietary. MDM software secures, monitors, manages, and supports a wide range of mobile devices.



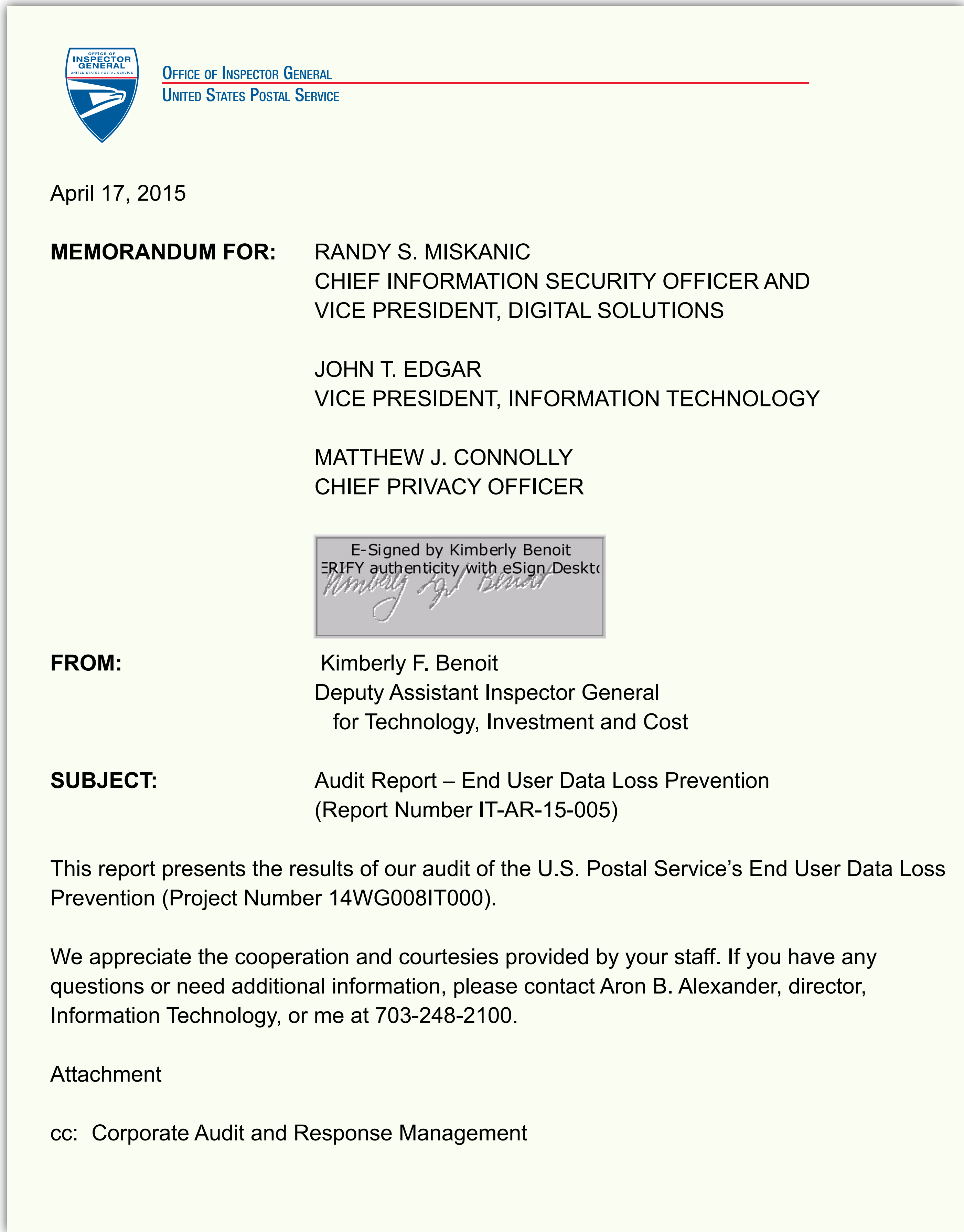
We determined that DLP and MDM systems could operate more effectively to prevent data loss from internal users within the Postal Service network.

Policies and Rules
Management could enhance current rules to prevent internal users from sending sensitive and sensitive-enhanced data outside the postal network.

Confidential Information in Documents
The Postal Service was not using the DLP system to its fullest extent to index proprietary and other business-sensitive information in documents.

Unencrypted eMails with Sensitive and Sensitive-enhanced Data (Outside of DLP Policies and Rules)
Internet
Network
DLP Server
Unindexed Documents With Highly Sensitive Corporate Data
Recordable Media
Exit
CLICK TO RESET

Transmittal Letter



OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

April 17, 2015

MEMORANDUM FOR: RANDY S. MISKANIC
CHIEF INFORMATION SECURITY OFFICER AND
VICE PRESIDENT, DIGITAL SOLUTIONS

JOHN T. EDGAR
VICE PRESIDENT, INFORMATION TECHNOLOGY

MATTHEW J. CONNOLLY
CHIEF PRIVACY OFFICER

E-Signed by Kimberly Benoit
ERIFY authenticity with eSign Deskto

FROM: Kimberly F. Benoit
Deputy Assistant Inspector General
for Technology, Investment and Cost

SUBJECT: Audit Report – End User Data Loss Prevention
(Report Number IT-AR-15-005)

This report presents the results of our audit of the U.S. Postal Service's End User Data Loss Prevention (Project Number 14WG008IT000).

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

Attachment

cc: Corporate Audit and Response Management

Table of Contents

Findings

We determined the DLP and MDM systems could operate more effectively to prevent data loss from internal users within the Postal Service network.

Introduction

This report presents the results of our audit of the U.S. Postal Service's End User Data Loss Prevention (Project Number 14WG008IT000). Our objective was to determine whether data loss prevention (DLP) and mobile device management (MDM) systems are operating effectively to prevent data loss from internal users within the Postal Service network. See Appendix A for additional information about this audit.

Data is often an organization's most valuable resource and the rise in data loss reflects the growing need for controls to prevent sensitive information from leaving a network. DLP systems help prevent internal users from maliciously or unintentionally leaking sensitive information, such as personally identifiable, financial or proprietary, and other business-sensitive information through email, the Internet, or portable devices. An effective DLP system should have data classifications that accurately describe the types of information that must be protected. In addition, DLP indexing[1] functionalities help prevent the leakage of highly sensitive information in documents.

The increasing use of personal computers and mobile devices requires agencies to develop new technologies to secure data. MDM software secures, monitors, manages, and supports a wide range of mobile devices. Smartphones and tablet computers can be deployed across mobile operators, service providers, and enterprises. By controlling and protecting the data and configuration settings for all mobile devices in the network, MDM reduces support costs and security risks.

Conclusion

We determined the DLP and MDM systems could operate more effectively to prevent data loss from internal users within the Postal Service network. Specifically, management could enhance DLP controls and implement MDM security controls to [redacted] These enhanced controls are not in place because management has not established formal DLP procedures to ensure continuous quality assurance testing for updating DLP policies and rules. In addition, management has not implemented a solution to enable the DLP system to [redacted] optional and not all of the business groups are aware of it. Further, management has not made it a priority to [redacted]

As a result, internal users could compromise sensitive employee, customer, and business information, which could lead to financial and legal consequences and negatively affect the Postal Service brand.

Data Loss Prevention System Controls

We determined that DLP systems could operate more effectively to prevent data loss from internal users within the Postal Service network. Intermittent testing of DLP policies and rules, the [redacted] could lead to leaked contract information or trade secrets and identity theft. This could cause serious financial and legal consequences for the Postal Service.

[1] Indexing is a form of "fingerprinting" a file or its contents that enables the DLP system to detect the presence of portions of a document. For example, a business unit may want to create an index to detect exact versions of sensitive information or the release of passages or sections of a document. The DLP policy and indexed passages or sections would be sent to the detection server for the system to compare file contents to fingerprints registered in the index file and identify matches.

Highlights
Table of Contents
Findings
Recommendations
Appendices

Policies and Rules

The Postal Service DLP system's [redacted] controls are working as designed by related policies and rules;[4] however, management could enhance current rules to prevent internal users from sending sensitive and sensitive-enhanced data outside the postal network. Sensitive information can include confidential business information, such as proprietary information and contractor bid or proposal information. Sensitive-enhanced data consists of credit card numbers and personally identifiable information, such as Social Security numbers.[5] There are no formal rules to ensure DLP policies are continuously reviewed, tested, and updated, even though Postal Service policy[6] requires the protection of sensitive and sensitive-enhanced information.

We conducted 55 tests[7] of the DLP's [redacted] and [redacted] policies and rules and identified one exception related to [redacted]. [redacted]

We conducted tests outside the DLP policies and rules that identified areas that management needs to enhance.

During this audit, management took actions that addressed this issue. Management blocked employees from accessing personal email providers from ACE workstations and prevented messaging functionality on the [redacted] website.

We conducted tests outside the DLP policies and rules that identified areas that management needs to enhance. Specifically:

- [redacted]
- [redacted]

[2] [redacted]

[4] A DLP policy combines detection rules and response actions. The policy rules are based on information security objectives.

[5] Handbook AS-805, *Information Security,* Sections 3-2.3.2 and 3-2.3.3, dated May 2014.

[6] According to Handbook AS-805, Sections 3.2.3.2 and 3.2.3.3, sensitive and sensitive-enhanced information needs the appropriate protection as warranted or required.

[7] We conducted these tests at a Postal Service facility using a computer on the Postal Service network. We conducted the following number of tests for each DLP component: [redacted]

[8] [redacted]

[9] The Postal Service uses [redacted] as its operating method to simplify, standardize, centralize, and efficiently manage its information technology (IT) environment.

[10] We obtained a temporary Postal Service email account to conduct our tests.

[11] We did not use actual credit card or social security numbers to conduct our tests. We used test data obtained from publicly available sources that resemble actual credit card and social security numbers.

[12] Keywords are specific words defined in DLP rules that identify sensitive-enhanced information.

[redacted]

The Postal Service has [redacted] for the DLP system to inspect or block encrypted email attachments for sensitive and sensitive-enhanced information before leaving the postal network. For example, the Postal Service's [redacted]. Best practices[14] recommend inspecting [redacted].

Confidential Information in Documents

The Postal Service was not using the DLP system to its fullest extent to index proprietary and other business-sensitive information in documents. DLP indexing services are optional; all business groups do not know the services exist and no formal process exists to ensure the groups that generate and maintain sensitive information are aware of existing DLP indexing services. Postal Service policy requires appropriate protection of sensitive information as warranted and required.

Postal Service policy requires appropriate protection of sensitive and sensitive enhanced information as warranted or required.

Mobile Device Management

[redacted] Test results also revealed [redacted]

Postal Service policy requires appropriate protection of sensitive and sensitive-enhanced information as warranted or required. In addition, [redacted] on organization-issued mobile devices. However, management has not made it a priority to implement effective mobile security controls that [redacted] In addition, management has not prevented internal users from accessing [redacted] applications and [redacted].

Without effective mobile security controls, internal users could compromise employee, customer, and business information, which could lead to financial and legal consequences associated with leaked contract information and trade secrets or identity theft.

[13] The Postal Service requires the use of [redacted].

[14] According to the CDW white paper, *Data Loss Prevention*, there are two work-arounds that allow inspection of [redacted]. One uses the network proxy server while emails are in transit and the other uses the capabilities of host-based DLP agents to inspect the information [redacted].

[15] [redacted]

Recommendations

We recommend the chief information security officer and Digital Solutions vice president:

1. Implement a formal data loss prevention process that involves conducting continuous quality assurance tests and reviewing and updating data loss prevention policies and rules.

2. Implement and communicate formal data loss prevention indexing processes and procedures to require business groups that generate and maintain sensitive information in documents to use data loss prevention indexing services.

We recommend the chief information security officer and Digital Solutions vice president consult with the chief privacy officer to:

3. Develop and implement a solution to enable the data loss prevention system [redacted]

We recommend the vice president, Information Technology, direct the manager, Enterprise Access Infrastructure, to coordinate with the chief information security officer and Digital Solutions vice president to:

4. Implement a mobile technology solution that [redacted] corporate data from being accessed by internal users through [redacted] and prevents internal users from accessing [redacted] applications and [redacted]

Management's Comments

Management agreed with our findings and recommendations and provided targeted implementation dates for addressing the issues in our report.

Management disagreed with our other impact calculations and stated that we presented no direct evidence of data loss in the report. Management also claimed that we did not base our assumptions for calculating the potential number of files lost on any standard industry-accepted benchmarks.

Regarding recommendation 1, management stated that they have taken steps to implement and enhance a DLP Quality Assurance testing program. Management stated that the targeted implementation date is April 30, 2015.

Regarding recommendation 2, management is targeting all Postal Career Executive Service level managers and above to increase awareness of the DLP indexing program technology available for protecting sensitive documents. Management stated that the targeted implementation date is June 30, 2015.

Regarding recommendation 3, management stated they have implemented the [redacted] solution to replace business-approved transmissions of sensitive information outside the Postal Service network in [redacted]. However, nationwide deployment of this capability will require phased updates to policy documents, training, and communications. Management stated that the targeted full implementation date is March 31, 2016.

Regarding recommendation 4, management is currently evaluating commercially available tools and plans to perform a proof-of-concept to recommend a best path forward by September 30, 2015.

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

Evaluation of Management's Comments

The U.S. Postal Service Office of Inspector General (OIG) considers management's comments responsive to the recommendations in the report.

In regard to management's disagreement with our other impact calculations, the overarching principle behind other impact is that it measures the amount of risk associated with uncertain events. Other impact does not state that the Postal Service will necessarily incur the loss or gain; however, it quantifies costs associated with lost sensitive data if management does not implement the suggested recommendations. To determine the adjusted cost per record, we used the Ponemon Institute's *2014 Cost of Data Breach Study: Global Analysis*, which is based on independent research concerning privacy, data protection, and information security policy. This analysis reports the public sector's direct and indirect expenses incurred in the event of a breach. We based the remainder of our calculations on a very conservative percentage (.01 percent of all outgoing emails) of sensitive information at risk directly related to the DLP and MDM findings in this report.

The OIG considers all recommendations significant, and therefore requires 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

Background

Two Postal Service groups manage the DLP and MDM systems. The Corporate Information Security Office manages DLP operations and Enterprise Access Infrastructure oversees the Mobile Computing group's management of mobile devices. Both groups are responsible for ensuring the protection of the Postal Service against data leakage by internal users.

The Postal Service's DLP system consists of five different components: [redacted] detect an average of about 1.1 million outbound email messages per day.[20] [redacted] servers detect information at Internet access points in [redacted] Agents installed on workstations manage DLP endpoint security. Similar security controls are in place to block content (such as credit card and Social Security numbers) for [redacted]. Incidents are sent to the DLP enforcement console. When an internal user violates a DLP policy, management sends that user an email with a reference to the violated policy.

The increasing use of personal computers and mobile devices has required agencies to develop new technologies, such as MDM software, to secure corporate data and minimize the risk of internal users leaking sensitive information. MDM software secures, monitors, manages, and supports a wide range of mobile devices deployed across the enterprise, including smartphones and tablet computers. If implemented and configured properly, MDM solutions can also reduce support costs and business security risks for all mobile devices in the network.

The Postal Service has deployed about 10,841 mobile devices[21] to internal users. It uses two MDM solutions to manage these devices: [redacted] and [redacted]. [redacted] was originally acquired to manage Blackberry® devices, but other mobile devices[23] have made it obsolete. [redacted] can support [redacted] devices and its console functions have more visibility and more advanced device management functions.

Objective, Scope, and Methodology

Our objective was to determine whether DLP and MDM systems are operating effectively to prevent data loss from internal users within the Postal Service network. To accomplish our objective, we:

- Met with Postal Service officials in Corporate Information Security, Network Performance Achievement, and Mobile Computing to document and understand the DLP and MDM systems; and with the privacy officer to document and understand related privacy matters.

- Reviewed and analyzed DLP policies and MDM rules for reasonableness.

- Developed and conducted DLP and MDM tests to determine whether DLP policies and MDM rules work as designed.

[18] [redacted]
[19] [redacted]
[20] Based on information provided on January 26, 2015, outbound emails for the previous 30 days totaled about 34 million.
[21] This total consists of about 6,947 iPhone, 3,446 Android, and 448 Blackberry® devices.
[22] Plans are to retire [redacted] because it cannot operate across multiple platforms.
[23] Includes iPhone, Samsung, and other Android devices.

- Compared DLP policies and MDM rules to best practices to identify areas for enhancement.
- Performed an access review to ensure that only appropriate personnel have access to the DLP system and the data it collects and contains.

We limited the scope of this audit to DLP and MDM controls related to the protection of sensitive information leaving the Postal Service network. Our assessment of DLP controls was exclusive to the DLP system and did not include a review of the results of scans and inventories of internal hard drives for identifying confidential data at rest. We also did not review other Postal Service environments where data could leave the Postal Service network without going through the DLP system[24] or assess controls around File Transfer Protocol servers. Finally, we limited our review of mobile device management activities to the mobile management roles, responsibilities, and controls related to preventing data loss by internal users.

We conducted this performance audit from August 2014 through April 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 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 March 16, 2015, and included their comments where appropriate.

We did not assess the reliability of any computer-generated data for the purposes of this report.

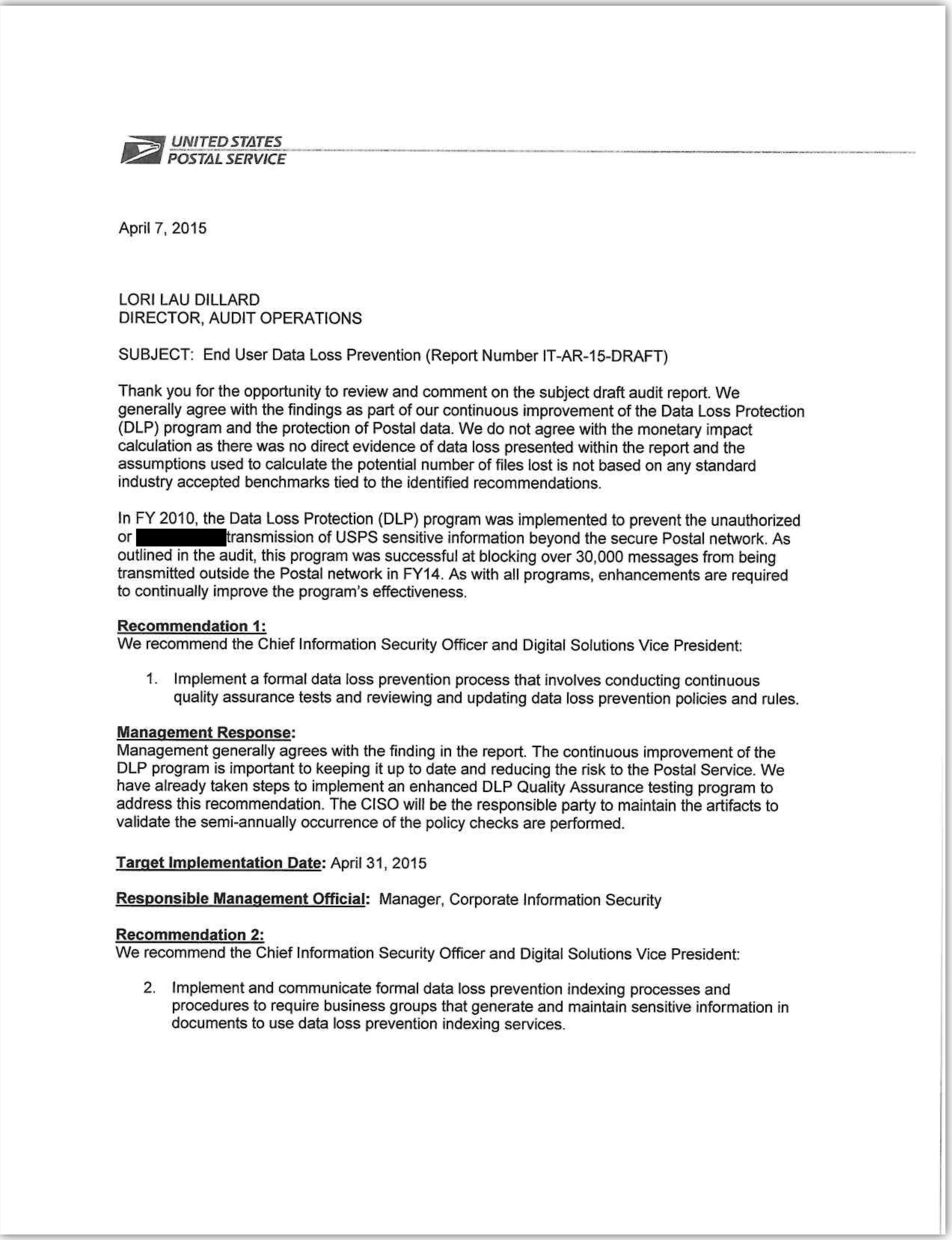
Prior Audit Coverage

Report Title	Report Number	Final Report Date	Monetary Impact
U. S. Postal Service Data Governance	DP-AR-13-004(R)	4/23/2013	None

Report Results: Our report determined the Postal Service could improve management of critical data to achieve strategic and operational goals. We identified 148 data-related issues in OIG reports issued in fiscal years 2009 through 2012, which included inconsistent corporate-wide data strategy, unreliable and inaccurate data, data inconsistencies within the Enterprise Data Warehouse, insufficient IT security measures, and difficulties with accessing and sharing data. Although the Postal Service defined a structure for a data governance program in 2003, full roles and responsibilities were not uniformly adopted across the enterprise. In addition, limitations in the Postal Service's data governance program placed the Postal Service at risk of potential vulnerabilities that could affect data quality, availability, and integrity. Our report outlined 34 industry data governance best practices the Postal Service should consider to foster and institutionalize a strong culture. We recommended the Postal Service implement a formal, enterprise-wide data governance program. Management agreed with the finding and recommendation.

[24] The Discovery component of the DLP systems conducts this activity.

Appendix B: Management's Comments



UNITED STATES
POSTAL SERVICE

April 7, 2015

LORI LAU DILLARD
DIRECTOR, AUDIT OPERATIONS

SUBJECT: End User Data Loss Prevention (Report Number IT-AR-15-DRAFT)

Thank you for the opportunity to review and comment on the subject draft audit report. We generally agree with the findings as part of our continuous improvement of the Data Loss Protection (DLP) program and the protection of Postal data. We do not agree with the monetary impact calculation as there was no direct evidence of data loss presented within the report and the assumptions used to calculate the potential number of files lost is not based on any standard industry accepted benchmarks tied to the identified recommendations.

In FY 2010, the Data Loss Protection (DLP) program was implemented to prevent the unauthorized or [redacted] transmission of USPS sensitive information beyond the secure Postal network. As outlined in the audit, this program was successful at blocking over 30,000 messages from being transmitted outside the Postal network in FY14. As with all programs, enhancements are required to continually improve the program's effectiveness.

Recommendation 1:
We recommend the Chief Information Security Officer and Digital Solutions Vice President:

1. Implement a formal data loss prevention process that involves conducting continuous quality assurance tests and reviewing and updating data loss prevention policies and rules.

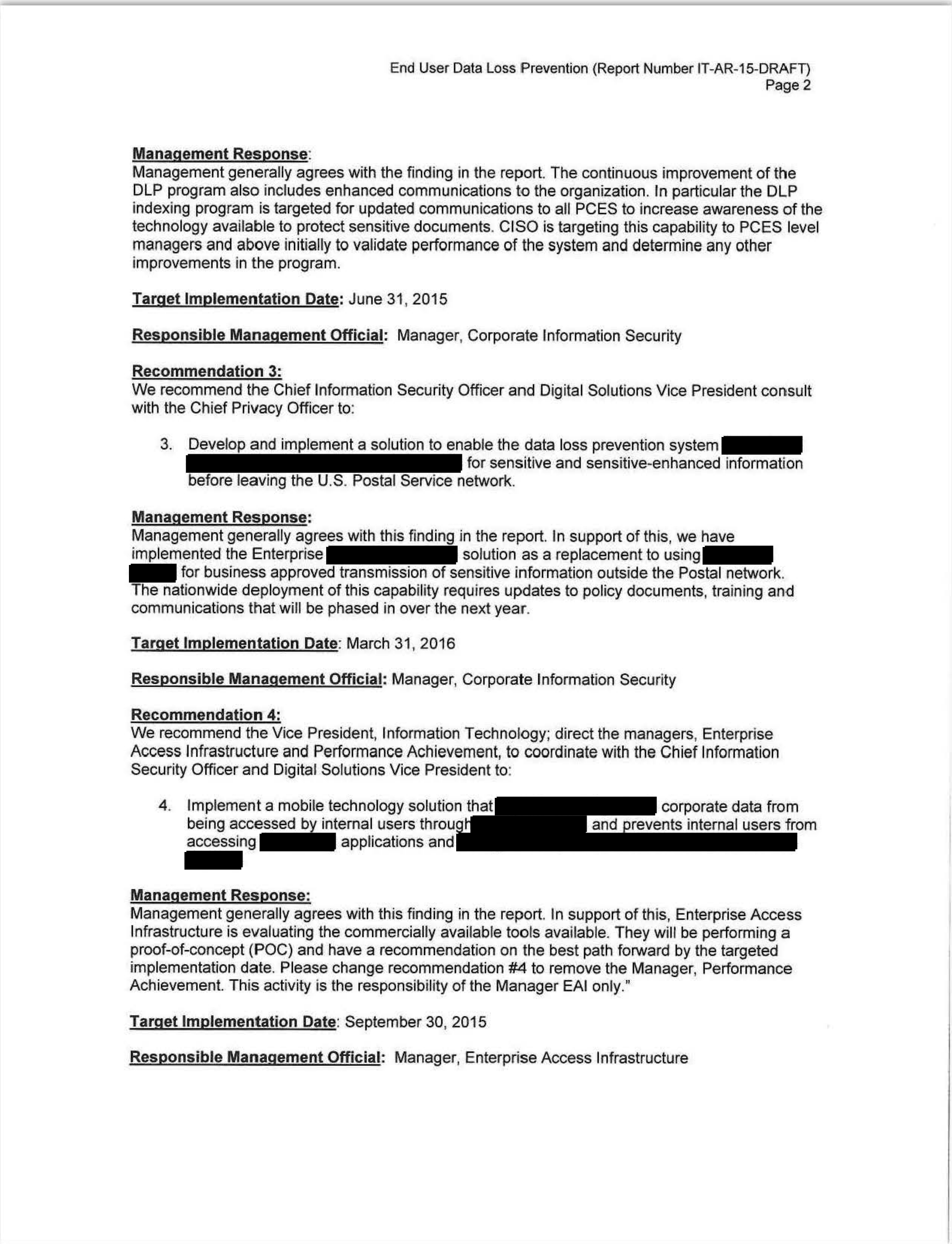
Management Response:
Management generally agrees with the finding in the report. The continuous improvement of the DLP program is important to keeping it up to date and reducing the risk to the Postal Service. We have already taken steps to implement an enhanced DLP Quality Assurance testing program to address this recommendation. The CISO will be the responsible party to maintain the artifacts to validate the semi-annually occurrence of the policy checks are performed.

Target Implementation Date: April 31, 2015

Responsible Management Official: Manager, Corporate Information Security

Recommendation 2:
We recommend the Chief Information Security Officer and Digital Solutions Vice President:

2. Implement and communicate formal data loss prevention indexing processes and procedures to require business groups that generate and maintain sensitive information in documents to use data loss prevention indexing services.



Management Response:
Management generally agrees with the finding in the report. The continuous improvement of the DLP program also includes enhanced communications to the organization. In particular the DLP indexing program is targeted for updated communications to all PCES to increase awareness of the technology available to protect sensitive documents. CISO is targeting this capability to PCES level managers and above initially to validate performance of the system and determine any other improvements in the program.

Target Implementation Date: June 31, 2015

Responsible Management Official: Manager, Corporate Information Security

Recommendation 3:
We recommend the Chief Information Security Officer and Digital Solutions Vice President consult with the Chief Privacy Officer to:

3. Develop and implement a solution to enable the data loss prevention system [redacted] for sensitive and sensitive-enhanced information before leaving the U.S. Postal Service network.

Management Response:
Management generally agrees with this finding in the report. In support of this, we have implemented the Enterprise [redacted] solution as a replacement to using [redacted] for business approved transmission of sensitive information outside the Postal network. The nationwide deployment of this capability requires updates to policy documents, training and communications that will be phased in over the next year.

Target Implementation Date: March 31, 2016

Responsible Management Official: Manager, Corporate Information Security

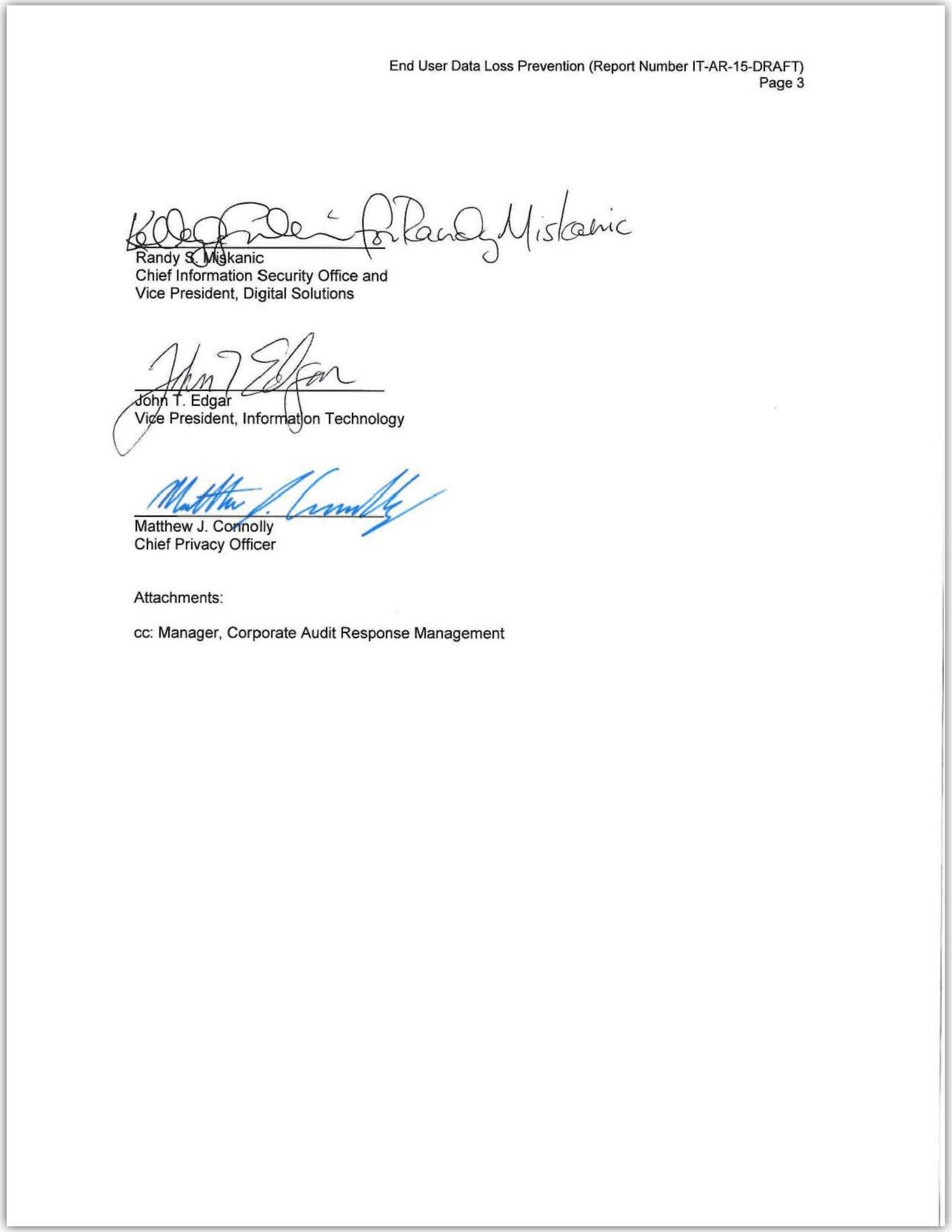
Recommendation 4:
We recommend the Vice President, Information Technology; direct the managers, Enterprise Access Infrastructure and Performance Achievement, to coordinate with the Chief Information Security Officer and Digital Solutions Vice President to:

4. Implement a mobile technology solution that [redacted] corporate data from being accessed by internal users through [redacted] and prevents internal users from accessing [redacted] applications and [redacted]

Management Response:
Management generally agrees with this finding in the report. In support of this, Enterprise Access Infrastructure is evaluating the commercially available tools available. They will be performing a proof-of-concept (POC) and have a recommendation on the best path forward by the targeted implementation date. Please change recommendation #4 to remove the Manager, Performance Achievement. This activity is the responsibility of the Manager EAI only."

Target Implementation Date: September 30, 2015

Responsible Management Official: Manager, Enterprise Access Infrastructure



for Randy Miskanic

Randy S. Miskanic
Chief Information Security Office and
Vice President, Digital Solutions

John T Edgar

John T. Edgar
Vice President, Information Technology

Matthew J. Connolly

Matthew J. Connolly
Chief Privacy Officer

Attachments:

cc: Manager, Corporate Audit Response Management

OFFICE OF
INSPECTOR
GENERAL
UNITED STATES POSTAL SERVICE

Contact us via our Hotline and FOIA forms, follow us on social networks, 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