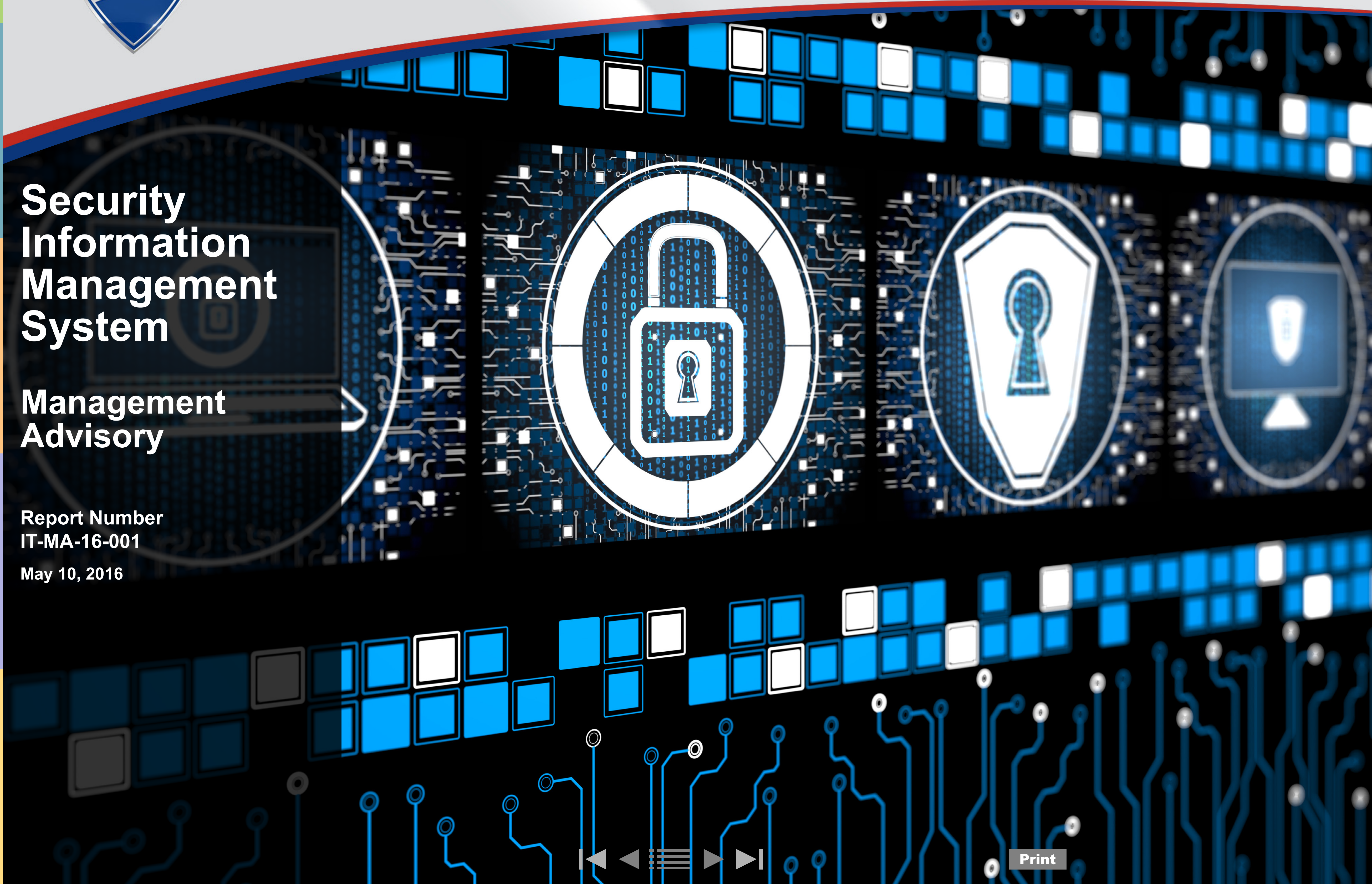
Highlights
Table of Contents
Findings
Recommendation
Appendices

OFFICE OF
INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE



Security Information Management System

Management Advisory

Report Number
IT-MA-16-001

May 10, 2016

Print

Highlights
Table of Contents
Findings
Recommendation
Appendices

OFFICE OF
INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

Highlights

Best practices for effective security controls include implementing processes that filter false positives from IT security event reporting. This enables security analysts to focus on legitimate and critical alerts.

Background

The U.S. Postal Service currently uses the [redacted] system to collect and analyze data on information technology (IT) security events, including malicious software referred to as malware. Each quarter, the U.S. Postal Service Office of Inspector General (OIG) analyzes [redacted] system data as part of our IT Security Risk Model. In Quarter (Q) 4, fiscal year (FY) 2015, the [redacted] system reported a [redacted] portion of security events as malware. However, these events were actually normal, expected behavior incorrectly labeled as malicious. Normal activity incorrectly labeled as malicious is referred to as false positives.

Best practices for effective security controls include implementing processes that filter false positives from IT security event reporting. This enables security analysts to focus on legitimate and critical alerts.

Our objective was to determine if the Postal Service properly configured its security information management system to exclude data that result in false positives.

What The OIG Found

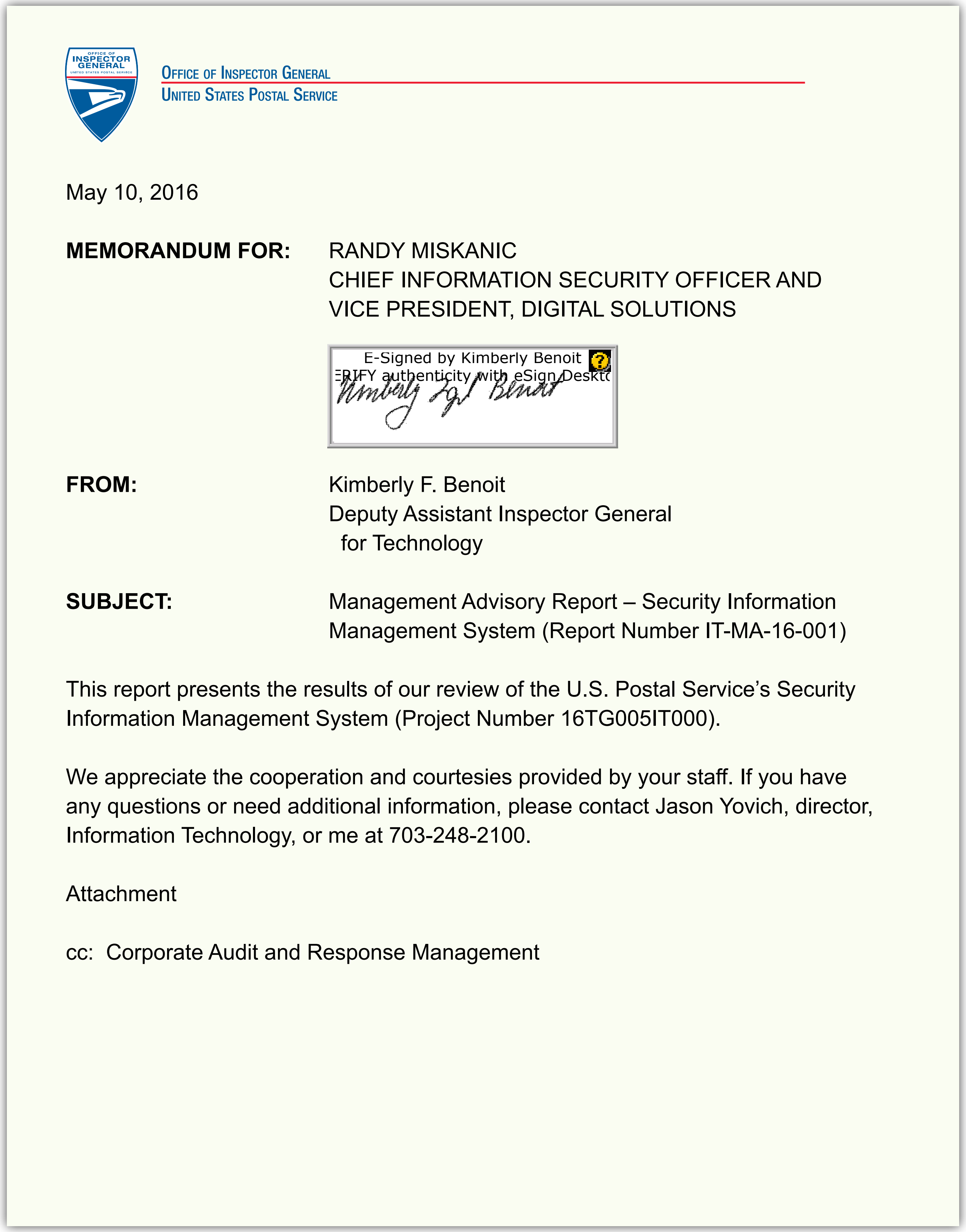
We determined that Postal Service IT security managers identified certain security events as false positives; however, they did not exclude them from [redacted] system data. In Q4, FY 2015, the [redacted] system reported about [redacted] malware events. We identified 10 programs that made up about 98 percent of these malware events.

IT security management stated they were aware that all but one of these programs were false positives based on earlier research, but did not remove them due to other priorities, such as implementing new tools and processes. As a result, false positives will continue to be reported as malware events in the [redacted] system.

What The OIG Recommended

We recommended the Postal Service establish procedures to regularly identify and manage false positives found in malware event reporting tools and incorporate these practices into the redesign of incident management and monitoring processes.

Transmittal Letter



OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

May 10, 2016

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

E-Signed by Kimberly Benoit
ERIFY authenticity with eSign Deskt

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

SUBJECT: Management Advisory Report – Security Information Management System (Report Number IT-MA-16-001)

This report presents the results of our review of the U.S. Postal Service's Security Information Management System (Project Number 16TG005IT000).

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

Attachment

cc: Corporate Audit and Response Management

Table of Contents

Highlights
Table of Contents
Findings
Recommendation
Appendices

Findings

Postal Service IT security management identified malware events as false positives; however, they did not exclude them from data in the [redacted] system.

Introduction

We are issuing this management advisory to provide U.S. Postal Service management with the results of our self-initiated review of the Postal Service's security information management system (Project Number 16TG005IT000). In Quarter (Q) 4, fiscal year (FY) 2015, the Postal Service's [redacted] system reported a [redacted] portion of malware events that were false positives.[1] Each quarter, the U.S. Postal Service Office of Inspector General (OIG) analyzes [redacted] system data as part of our Information Technology (IT) Security Risk Model. The objective of this review was to determine if the Postal Service's security information management system was properly configured to exclude data that result in false positives. See Appendix A for additional information about this review.

The Postal Service currently uses the [redacted] system to collect and analyze data on IT security events, including malware. Shortly after we began our review, managers reporting to the chief information security officer began initiatives to restructure Postal Service processes and develop new ways to monitor IT security events.[2]

The Center for Internet Security's (CIS) *Critical Security Controls for Effective Cyber Defense*[3] addresses the importance of having processes to filter out normal or expected data so security analysts can spend time on legitimate and critical alerts or events. In addition, a 2015 Enterprise Strategy Group report showed that 28 percent of organizations surveyed said their enterprise had too many false positive alerts.[4]

Summary

We determined that Postal Service IT security management identified malware events as false positives; however, they did not exclude them from data in the [redacted] system. IT security management stated they were aware, based on earlier research, that the false positives identified as malware were not security risks. Management stated that the reason for leaving false positives in the data was because they wanted to use resources to implement new IT security tools and processes. Therefore, false positives will continue to be reported as malware events in the [redacted] system.

False Positives

In Q4, FY 2015, the [redacted] system reported [redacted] malware events from [redacted] identified program files. We reviewed the ten most frequent program files, which represented about 98 percent of total reported malware events, and found that [redacted] were false positives.[5] Figure 1 identifies the programs we reviewed and provided to Postal Service IT security management to confirm they were false positives.

[1] Any normal or expected behavior that is identified as malicious. Part of the art of event management is minimizing false positives without blinding the organization to relevant attacks.

[2] Details and funding levels for management's plan are in the decision analysis report (DAR) titled *Cybersecurity Improvements DAR-II,* dated July 27, 2015.

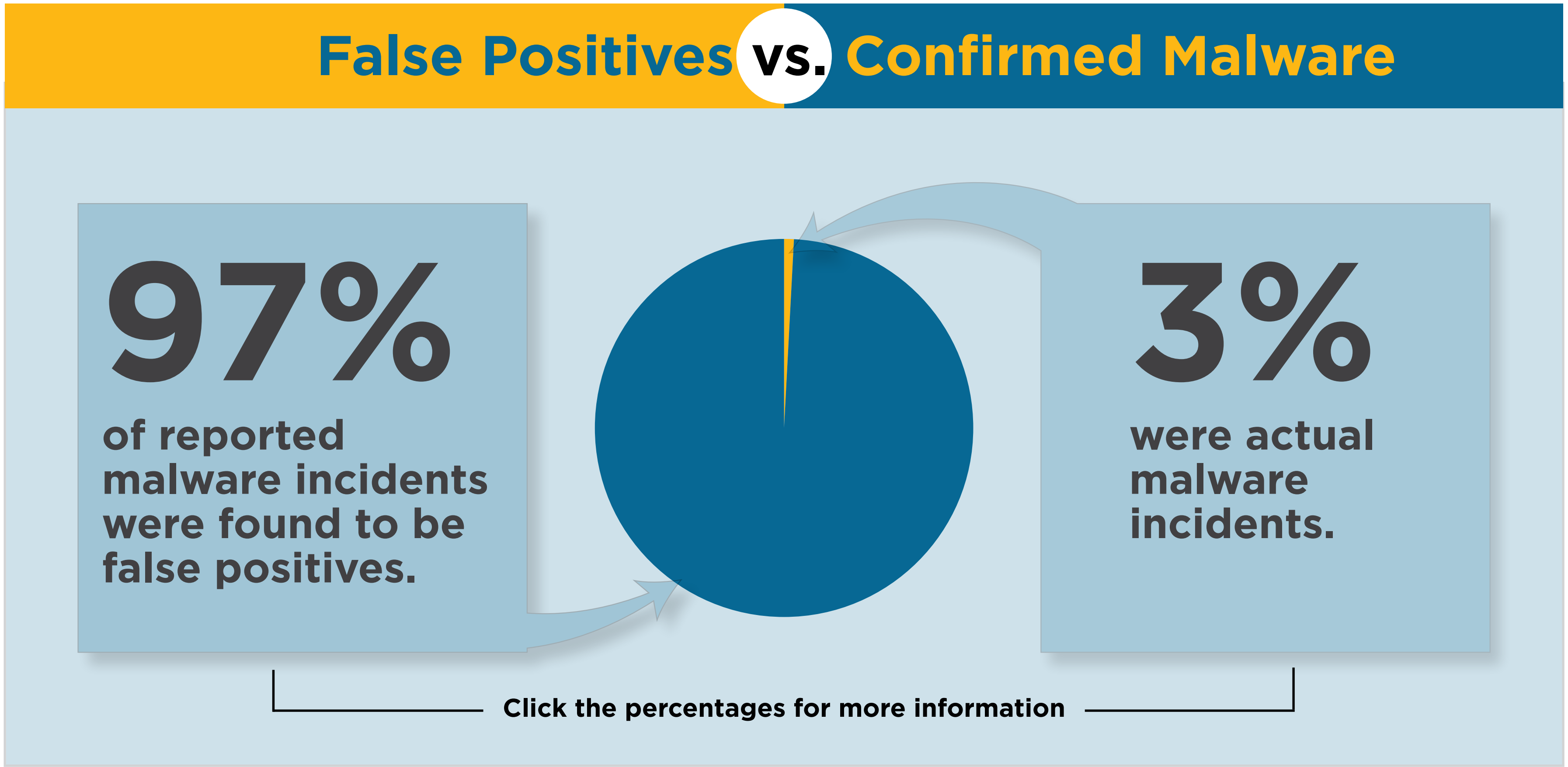
[3] Critical Security Control 6: Maintenance, Monitoring, and Analysis of Audit Logs, Version 6, October 15, 2015.

[4] *An Analytics-Based Approach to Cybersecurity,* Jon Oltsid, dated May 2015. The Enterprise Strategy Group is a private company that provides research on security information and trends throughout the IT community.

[5] There were [redacted] occurrences or events combined for the ten program files reviewed.

> ***According to best practices, security incident data should be reduced so analysts can understand and identify events of interest.***

Figure 1: Programs Selected for Review



False Positives vs. Confirmed Malware

97% of reported malware incidents were found to be false positives.

3% were actual malware incidents.

Click the percentages for more information

Source: Postal Service [redacted] system data for Q4, FY 2015 and OIG analysis.

Postal Service IT security managers researched the ten programs reported as malware and confirmed that [redacted] were false positives.[6] For example, program number. 2 is a monitoring program the Postal Service uses for its self-service retail kiosks. The [redacted] false positive programs comprised 97 percent of total malware in Q4, FY 2015. IT security managers stated these [redacted] programs were not security risks, but did not eliminate them from [redacted] system data. This occurred because management decided to use available resources to implement new IT security tools and processes.[7] Therefore, these programs continued to be reported as malware events in the [redacted] system during Q1, FY 2016, despite the fact that they were false positives.

According to best practices, security incident data should be reduced so analysts can understand and identify events of interest.[8] In addition, administrators and security personnel should fine tune detection to focus on unusual activity, avoid false positives, and prevent overwhelming analysts with insignificant alerts.[9] Consequently, we believe incorporating these best practices to eliminate false positives from malware events would enhance IT security. Currently, IT security management is restructuring its processes and reviewing best practices regarding malware incident management and monitoring.

[6] [redacted].
[7] The Postal Service is investing additional resources to strengthen the monitoring, detection, and analytic capabilities of its computing environment with spending increases for cybersecurity projects in FYs 2016 and 2017.
[8] SANS™ Institute publication, *Distilling Data in a SIM: A Strategy for the Analysis of Events in the ArcSight ESM* (Enterprise Security Manager), James Voorhees, September 26, 2007.
[9] The CIS *Critical Security Controls for Effective Cyber Defense*.

Recommendation

We recommend the chief information security officer and vice president, Digital Solutions, direct the manager, Cybersecurity Operations, to:

1. Establish procedures to regularly identify and manage false positives found in malware event reporting tools and incorporate these practices into the redesign of incident management and monitoring processes.

We recommend management establish procedures to regularly identify and manage false positives found in malware event reporting tools and incorporate these practices into the redesign of incident management and monitoring processes.

Management's Comments

Management agreed with the finding and recommendation.

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

Management stated they are currently restructuring malware incident management and monitoring processes and replacing the existing security information management system as part of a multi-phased cybersecurity strategy. This restructuring and replacement effort will incorporate best practices to better identify and manage false positives. The target implementation date is December 30, 2016.

Evaluation of Management's Comments

The OIG considers management's comments responsive to the recommendation and corrective actions should resolve the issues identified in the advisory.

The OIG agrees that the Postal Service's planned initiative to incorporate best practices in the restructuring of malware incident management and monitoring processes and replace the [redacted] system should resolve the issue we identified.

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

Appendices

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

Highlights
Table of Contents
Findings
Recommendation
Appendices

Appendix A: Additional Information

Background

The Postal Service uses the [redacted] system to monitor network and system activity. The software collects data from devices such as workstations, computer servers, and intrusion detection systems; and presents the data in the form of alerts to IT security managers in Raleigh, NC. Management must make an assessment as to whether or not an alert is caused by normal or expected activity. When normal activity is reported as though it was malicious activity, the alert is considered a false positive.

Each quarter, the OIG uses its IT Security Risk Model to analyze [redacted] system data for antivirus security events and potentially malicious inbound emails detected on devices on the Postal Service's nationwide network. The risk model for Q4, FY 2015, disclosed that a [redacted] portion of [redacted] system malware events were false positives. Given the [redacted] volume of alerts reported by the [redacted] system, false positives in the data can make it difficult for IT security analysts to identify important and critical events that warrant research or action. The problem of false positives in security management data is not specific to the Postal Service as many organizations encounter it.

The importance of malware detection and analysis tools continues to increase as threats to cybersecurity grow. To combat these growing threats, the Postal Service is investing additional resources to strengthen the monitoring, detection, and analytic capabilities of its computing environment. A 2015 DAR[10] details the planned spending increases for 15 cybersecurity projects in FY 2016 and FY 2017. The objective of the Incident Management, Control, and Response project is to develop the ability to identify and analyze events, detect incidents, and determine appropriate organizational responses over the next 2 years.

Objective, Scope, and Methodology

Our objective was to determine if the Postal Service's [redacted] system was properly configured to exclude data that result in false positives. We limited the scope of this review to the malware event data the [redacted] system reported in Q4, FY 2015.

To accomplish our objective, we

- Obtained an understanding of the [redacted] system and related flow of information;
- Researched the use of the [redacted] system in Postal Service environments;
- Analyzed total malware events reported in Q4, FY 2015, to determine how frequent each of the source files appeared during the period; and
- Researched industry best practices for the operation, maintenance, and configuration of security information management systems.

We conducted this review from December 2015 through May 2016, 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 work to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our objective. We believe that the evidence obtained provides a reasonable basis for our finding and conclusion based on our audit objective. We discussed our observations and conclusion with management on April 7, 2016, and included their comments where appropriate.

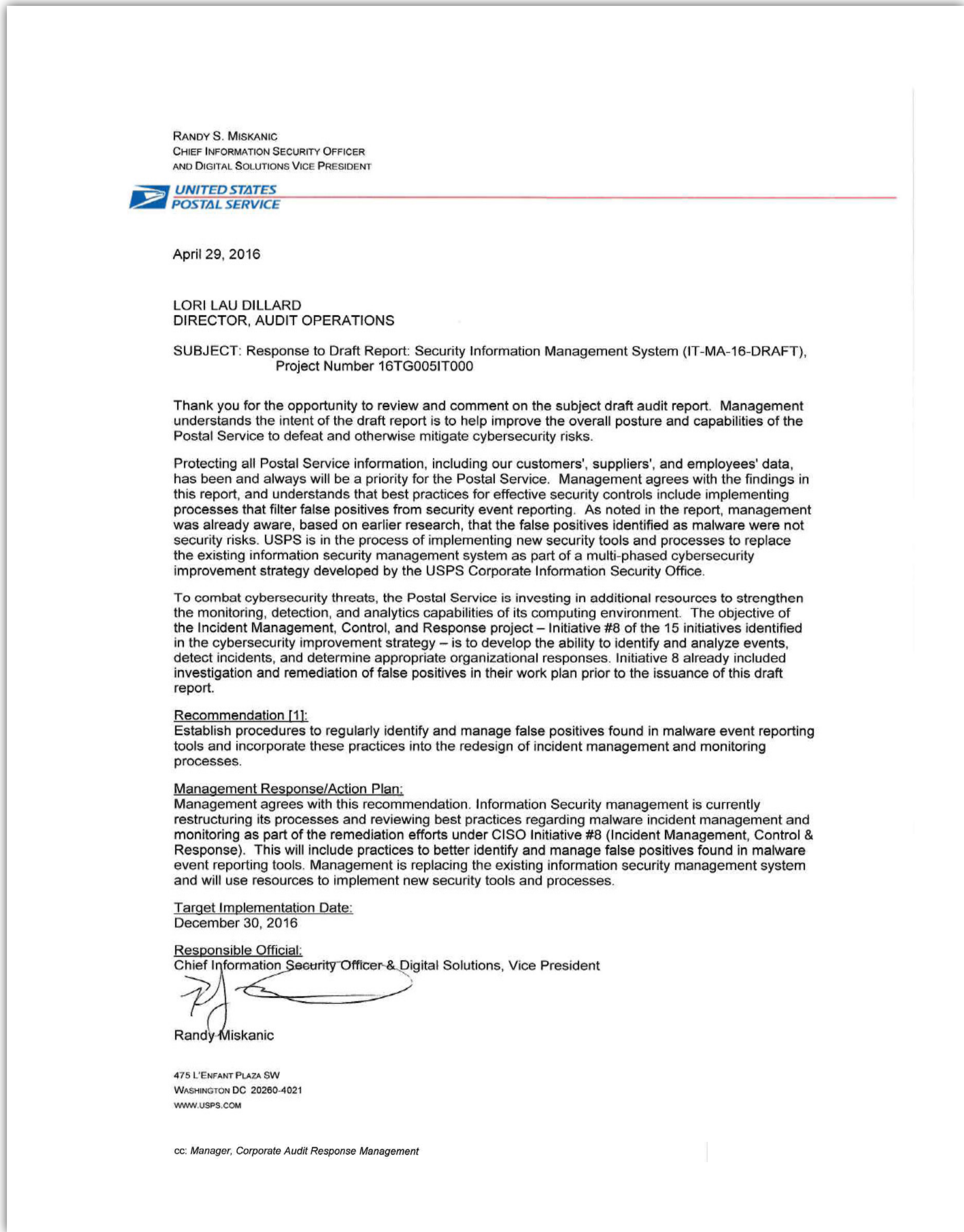
[10] *Cybersecurity Improvements DAR-II*, dated July 27, 2015.

We assessed the reliability of malware event data reported by the [redacted] system by reviewing related software documentation and interviewing IT security managers. We determined that the data was sufficiently reliable for the purposes of this report.

Prior Audit Coverage

The OIG did not identify any prior audits or reviews related to the objective of this advisory.

Appendix B: Management's Comments



RANDY S. MISKANIC
CHIEF INFORMATION SECURITY OFFICER
AND DIGITAL SOLUTIONS VICE PRESIDENT

UNITED STATES
POSTAL SERVICE

April 29, 2016

LORI LAU DILLARD
DIRECTOR, AUDIT OPERATIONS

SUBJECT: Response to Draft Report: Security Information Management System (IT-MA-16-DRAFT), Project Number 16TG005IT000

Thank you for the opportunity to review and comment on the subject draft audit report. Management understands the intent of the draft report is to help improve the overall posture and capabilities of the Postal Service to defeat and otherwise mitigate cybersecurity risks.

Protecting all Postal Service information, including our customers', suppliers', and employees' data, has been and always will be a priority for the Postal Service. Management agrees with the findings in this report, and understands that best practices for effective security controls include implementing processes that filter false positives from security event reporting. As noted in the report, management was already aware, based on earlier research, that the false positives identified as malware were not security risks. USPS is in the process of implementing new security tools and processes to replace the existing information security management system as part of a multi-phased cybersecurity improvement strategy developed by the USPS Corporate Information Security Office.

To combat cybersecurity threats, the Postal Service is investing in additional resources to strengthen the monitoring, detection, and analytics capabilities of its computing environment. The objective of the Incident Management, Control, and Response project – Initiative #8 of the 15 initiatives identified in the cybersecurity improvement strategy – is to develop the ability to identify and analyze events, detect incidents, and determine appropriate organizational responses. Initiative 8 already included investigation and remediation of false positives in their work plan prior to the issuance of this draft report.

Recommendation [1]:
Establish procedures to regularly identify and manage false positives found in malware event reporting tools and incorporate these practices into the redesign of incident management and monitoring processes.

Management Response/Action Plan:
Management agrees with this recommendation. Information Security management is currently restructuring its processes and reviewing best practices regarding malware incident management and monitoring as part of the remediation efforts under CISO Initiative #8 (Incident Management, Control & Response). This will include practices to better identify and manage false positives found in malware event reporting tools. Management is replacing the existing information security management system and will use resources to implement new security tools and processes.

Target Implementation Date:
December 30, 2016

Responsible Official:
Chief Information Security Officer & Digital Solutions, Vice President

Randy Miskanic

475 L'ENFANT PLAZA SW
WASHINGTON DC 20260-4021
WWW.USPS.COM

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.
Stay informed.

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