Highlights
Table of Contents
Findings
Recommendations
Appendices

OFFICE OF
INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

U.S. Postal Service Mass Data Compromise Response Plan

Audit Report

Report Number
IT-AR-16-002

December 7, 2015

Print

OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

Highlights

The Mass Data Compromise Response Plan (MDCRP) was developed in fiscal year 2010 to enable the Postal Service to respond to the threat of cyber intrusions.

Background

The U.S. Postal Service has one of the world's largest computer networks, which enables nationwide communication among more than 32,000 facilities. Over 500,000 employees work at these facilities, processing and delivering almost 155 billion mail pieces annually. In addition, the computer network stores, transmits, and processes financial, employee, contractor, and vendor information.

The Mass Data Compromise Response Plan (MDCRP) was developed in fiscal year 2010 to enable the Postal Service to respond to the threat of cyber intrusions. It defines the roles and responsibilities of response team members, specifies incident severity levels, outlines the process flow for incident management, and provides methodologies for conducting response activities. The Corporate Information Security Office (CISO) maintains and updates the MDCRP.

In October 2014, the CISO used four of the six sections of the MDCRP to respond to a cyber intrusion. These included the command structure, risk assessment, notification, and reporting sections. The remaining two sections, incident response and assessment, were not used during the 2014 cyber intrusion because the plan was not originally designed to respond to external cyber intrusions.

Since early November 2014, the chief information officer and supporting management continued mitigating the cyber intrusion by upgrading computer systems, removing compromised servers and workstations, implementing additional security monitoring, limiting remote user access, and blocking access to personal email sites.

Our objective was to assess the sufficiency and implementation of the Postal Service's MDCRP in response to the 2014 cyber intrusion.

What the OIG Found

Although the plan provided some guidance when the intrusion occurred, it needs to be updated to reflect best practices and to align with USPS policy. Specifically, the MDCRP did not have a security clearance requirement for groups such as the CISO or the Privacy and Records Office for responding to events that involve sensitive information. In addition, the MDCRP was missing five key elements: critical assets, comprehensive workflow processes, incident checklists, external communication protocols, and a Postal Service policy. Finally, the Postal Service tested the MDCRP only three times over the last 6 years.

According to the CISO technical service manager, this occurred because the MDCRP focused on internal employee threats rather than external sophisticated attacks. In addition, CISO did not annually test the plan as recommended by industry best practice. The Postal Service is currently working to improve its response capabilities and intends to update the plan once some of those improvements are in place.

In addition, the CISO had challenges in effectively evaluating the extent of the cyber intrusion as required by the plan because it did not have the appropriate technology and services, such as forensic investigation services. Since the 2014 cyber intrusion, the Postal Service has started corrective action to identify and acquire the technologies and services required to better respond to and remediate future cyber intrusions.

The Postal Service approved two financial requests, one in February and one in July 2015, for technology and services required to address a cyber intrusion. The first financial request was for critical and immediate cyber intrusion activities. As part of this request, the Postal Service implemented technologies such as new hardware and software to increase control over critical applications and deployment of monitoring and intrusion detection software.

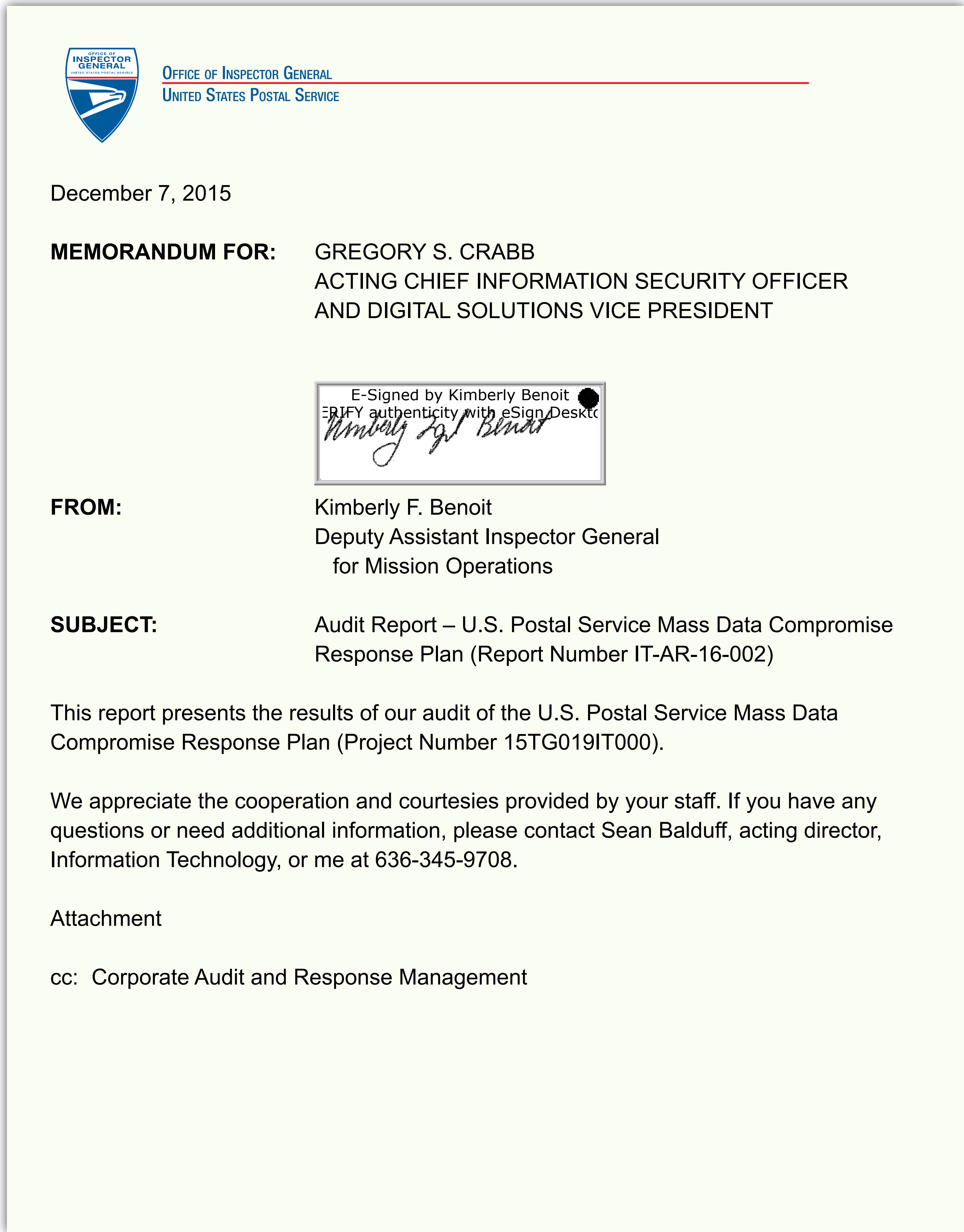
The second financial request provides for a more robust security posture for the organization such as expanding the CISO and improving cybersecurity awareness and training.

The acting manager, CISO, said the plan will be updated after the CISO receives the results of the October 2015 testing and the findings and recommendations from this audit. An updated plan must include, at a minimum, critical information technology assets, comprehensive workflow processes, incident checklists, external communication protocols, Postal Service policy requirements, and annual testing. A comprehensive plan will ensure the Postal Service is better prepared to respond to future cyber intrusions.

What the OIG Recommended

We recommended the Postal Service update its MDCRP to incorporate external cyber intrusion threats and include a security clearance requirement for employees. We also recommended CISO add the five key elements that are missing from the plan and test it at least annually.

Transmittal Letter



Office of Inspector General
United States Postal Service

December 7, 2015

MEMORANDUM FOR: GREGORY S. CRABB
ACTING CHIEF INFORMATION SECURITY OFFICER
AND DIGITAL SOLUTIONS VICE PRESIDENT

E-Signed by Kimberly Benoit
ERIFY authenticity with eSign Deskto

FROM: Kimberly F. Benoit
Deputy Assistant Inspector General
for Mission Operations

SUBJECT: Audit Report – U.S. Postal Service Mass Data Compromise Response Plan (Report Number IT-AR-16-002)

This report presents the results of our audit of the U.S. Postal Service Mass Data Compromise Response Plan (Project Number 15TG019IT000).

We appreciate the cooperation and courtesies provided by your staff. If you have any questions or need additional information, please contact Sean Balduff, acting director, Information Technology, or me at 636-345-9708.

Attachment

cc: Corporate Audit and Response Management

Table of Contents

Findings

Currently, the MDCRP does not align with Postal Service Handbook AS-805, Information Technology, or industry best practices.

Introduction

This report presents the results of our audit of the U.S. Postal Service Mass Data Compromise Response Plan (MDCRP) (Project Number 15TG019IT000). Our objective was to assess the adequacy and implementation of the MDCRP in response to the Postal Service's November 2014 cyber intrusion. See Appendix A for additional information about this audit.

The purpose of the MDCRP is to clarify the steps required to protect the Postal Service's information assets, employee information, and brand. The Corporate Information Security Office (CISO) maintains and updates the MDCRP.

The Postal Service has one of the world's largest computer networks, which enables nationwide communication among more than 32,000 facilities. Over 500,000 employees work at these facilities, processing and delivering almost 155 billion mail pieces annually. In addition, the computer network stores, transmits, and processes financial, employee, contractor, and vendor information.

The Postal Service developed the MDCRP during fiscal year (FY) 2010 to enable the Postal Service to respond to the threat of cyber intrusions. The MDCRP provides a strategy to address cyber intrusions, defines the roles and responsibilities for response team members, specifies incident severity levels, outlines the process flow for incident management, and provides methodologies for conducting response activities. The MDCRP applies to Postal Service information technology (IT) services — including all computer systems and applications — as well as cloud services.

In October 2014, CISO used four of the six sections of the MDCRP to respond to the cyber intrusion. These included the command structure, risk assessment, notification, and reporting sections. According to the CISO technical service manager, the remaining two sections — incident response and assessment — were not used during the 2014 cyber intrusion because the plan was not originally designed to respond to external cyber intrusions.

Since early November 2014, the chief information officer and supporting management continued mitigating the cyber intrusion by upgrading computer systems, removing compromised servers and workstations, implementing additional security monitoring, limiting remote user access, and blocking access to personal email sites.

Summary

Currently, the MDCRP does not align with Postal Service Handbook AS-805, *Information Technology*, or industry best practices. Specifically, the MDCRP did not have a security clearance requirement for groups such as CISO or the Privacy and Records Office to respond to events involving sensitive information. In addition, the MDCRP was missing five key elements: critical assets, comprehensive workflow processes, incident checklists, external communication protocols, and Postal Service policy requirements. Furthermore, the Postal Service tested the MDCRP only three times over the last 6 years. The Postal Service is working to improve its response capabilities, and intends to update the plan, once some of those improvements are in place.

According to the CISO technical service manager, this occurred because the MDCRP focused on internal employee threats rather than external sophisticated attacks. In addition, the CISO did not annually test the plan as recommended by industry practice.

CISO did not have the appropriate technology and services, such as forensic investigation services to evaluate the extent of the cyber intrusion, to meet MDCRP requirements. Since the 2014 cyber intrusion, the Postal Service has started corrective action to identify and acquire the technologies and services required to better respond and remediate future cyber intrusions.

The Postal Service approved two financial requests, one in February and one in July 2015, for technology and services required to address a cyber intrusion. The first financial request was for critical and immediate cyber intrusion activities. As part of this request, the Postal Service implemented technologies such as new hardware and software to increase control over critical applications and deployment of monitoring and intrusion detection software.

The second financial request provides for a more robust security posture for the organization such as expanding CISO and improving cybersecurity awareness and training.

The acting manager, CISO, said the MDCRP will be updated after the CISO receives the results of the October 2015 MDCRP testing and the findings and recommendations from this audit. An updated MDCRP, at a minimum, must include critical IT assets, comprehensive workflow processes, incident checklists, external communication protocols, Postal Service policy requirements, and annual testing. A comprehensive MDCRP will ensure the Postal Service is better prepared to respond to future cyber intrusions.

Plan Sufficiency and Implementation

At the time of the 2014 cyber intrusion, the MDCRP did not align with Handbook AS-805 or industry best practices because it focused on internal employee threats rather than external sophisticated attacks.

Security Clearances

The MDCRP did not have a security clearance requirement for groups such as CISO or the Privacy and Records Office to respond to events that involve sensitive information.

The MDCRP did not have a security clearance requirement for groups such as CISO or the Privacy and Records Office to respond to events that involve sensitive information. As of September 2015, 16 of 28 key personnel had security clearances. According to the acting manager, CISO, in July 2015 management started an initiative to review job descriptions to determine security clearance requirements. However, there is no estimated timeline for completing this initiative.

Plan Elements

The Postal Service's MDCRP needs to incorporate these five key elements[1]:

Create a list of the Postal Service's critical data, assets, and services that require the most protection during a cyber intrusion. The Postal Service would use this list to prioritize what mission critical data, assets, and services are at the greatest risk.

Develop comprehensive workflow processes, procedures, and flowcharts for responding to cyber incidents. According to best practices, processes, procedures, and flowcharts should include enough detail to ensure a proper cyber intrusion response.

Create incident handling and remediation checklists to ensure that the steps in the MDCRP response are followed during a cyber incident, for example, steps for incident identification, eradication, and recovery.[2] According to best practices, checklists should provide a clear set of steps to take during a cyber intrusion.

Specify protocols for communicating incidents with external agencies, such as the Department of Homeland Security and the FBI. These communications often need to occur quickly, so the Postal Service should set communication guidelines so it can share appropriate information with the right parties.

Incorporate critical Postal Service policy requirements, such as recertification and accreditation[3] for affected infrastructure[4] and applications[5] into the MDCRP. It is essential to test, monitor, and validate the systems prior to placing them back into production to verify they were not compromised in any other way.

CLEAR SHOW ALL

According to the acting manager, CISO, the CISO agrees that these elements are missing and will add them to the MDCRP. As of July 2015, Postal Service management had received feedback from After Action Reports[6] on improvements the MDCRP needs. In addition, the acting manager, CISO, said the MDCRP will be updated after the CISO receives the results of the October 2015

[1] The five elements are based on best practices in the SANS Institute InfoSec Reading Room, *The Incident Handler's Handbook*, December 5, 2011; NIST SP 800-61, Revision 2; *Computer Security Incident Handling Guide*, August 2012; Handbook AS-805-A, Information Resource Certification and Accreditation Process, Section 6-2.j; and Handbook AS-805-B, *Infrastructure Information Security Assurance (ISA) Process*, Section 5-2.b.

[2] According to the SANS Institute InfoSec Reading Room, The Incident Handler's Handbook, December 5, 2011; and NIST SP 800-61, Revision 2, *Computer Security Incident Handling Guide*, August 2012.

[3] The Certification & Accreditation (C&A) process is a formal security analysis and management approval process used to assess residual risk before a system is put into production.

[4] Handbook AS-805-A, Section 6-2.j, Criteria Forcing Security Recertification, dated March 2015.

[5] Handbook AS-805-B, Section 5-2.b, When Re-ISA Is Required, dated March 2005.

[6] Carnegie Mellon University, Software Engineering Institute, *Postal Service September 2014 Cyber Intrusion Incident After Action Report*, February 2015; and Raytheon Blackbird Technologies, Inc., *Technical Security Assessment of the USPS, After Action and Information Security Report*, June 2015.

MDCRP testing and the findings and recommendations from this audit. The CISO will need to integrate these key elements into the MDCRP to ensure the Postal Service is adequately prepared to address future cyber intrusions.

Testing of the Mass Data Compromise Response Plan

The Postal Service tested the MDCRP only three times over the last 6 years. According to industry best practices,[7] a response plan should be tested at least annually with the entire incident response team. According to the CISO technical service manager, this occurred because the CISO did not have sufficient staff to perform proper testing of the plan. According to the acting manager, CISO, the Postal Service plans to perform testing in October 2015. If the MDCRP is not tested annually, the Postal Service will not be adequately prepared to respond effectively to future cyber intrusions. Table 1 summarizes results from the last three MDCRP tests.

Table 1. Summary of MDCRP Test Results

Test Date	Test Name	Test Scenario	Relevant Test Results
May 2009[8]	Mass Data Breach Tabletop[9] Exercise	Mass Data Breach	The test identified the need for a comprehensive MDCRP.
September 2010	Cyber Storm III	Spoof[10] USPS.com website	This test concluded that regular testing and review of cyber incident response policies and procedures are necessary to protect Postal Service assets.
August 2014	August 2014 Incident Response Table Top Exercise	Distributed Denial of Service Attack[11]	The exercise recommended performing detailed testing to help incorporate feedback and requirements from the broader stakeholder community.

Source: Postal Service.

CISO management did not have the appropriate technology and services, such as forensic investigation services to evaluate the extent of the cyber intrusion or specialized hardware and software to analyze a cyber intrusion.

Technology and Services

CISO management did not have the appropriate technology and services, such as forensic investigation services to evaluate the extent of the cyber intrusion or specialized hardware and software to analyze a cyber intrusion. This is important because the appropriate technology and services in combination with the MDCRP will be needed when a future cyber intrusion is detected. According to the CISO technical service manager, CISO did not have sufficient staff available to determine the technology and services required to effectively analyze and respond to significant cyber intrusions.

Since the 2014 cyber intrusion, the Postal Service has started corrective action to identify and acquire the technologies and services it needs to better respond to and remediate future cyber intrusions.

[7] According to an analyst at Gartner, Inc.® (Gartner), a leading IT research and advisory company.
[8] The Postal Inspection Service developed a pre-cursor to the MDCRP that it tested in 2009.
[9] An exercise designed to test the theoretical ability of a group to respond to a situation.
[10] Spoofing is when a malicious party impersonates another user on a network to launch attacks against a network, steal data, or bypass access controls.
[11] A multitude of compromised systems work together to attack a single target, causing services to become unavailable for users of the targeted system.

The Postal Service approved two decision analysis reports (DAR)[12] in 2015 — one in February and one in July — for new technology and services. The February 2015 DAR requested $74.2 million for critical and immediate cyber intrusion activities. As part of this request, the Postal Service implemented technologies such as new hardware and software to increase control over critical applications and deployed monitoring and intrusion detection software. The July 2015 DAR requested $186 million to provide a more robust security posture for the organization, such as expanding CISO staff with a mix of contractors and additional staff, improving cybersecurity awareness, and training.

Because the Postal Service is acquiring the needed technology and services to respond to cyber intrusions, we are not making a recommendation on this matter.

[12] DAR Business Case Cyber Security FN 67-0287, FN 68-0192, February 20, 2015; and FN 68-2025, July 27, 2015. The February DAR shows that the Postal Service invested $8.7 million to support the remediation of the 2014 cyber intrusion, including technologies and services; and $65.5 million to support implementation of security enhancements. The July DAR shows an investment of $186 million to support continued enhancement and implementation of Postal Service information security technology, processes, and supporting organizational capabilities.

Recommendations

We recommend management update the MDCRP to include an external cyber focus and the five key elements; and annually test the MDCRP plan in accordance with industry best practices.

We recommend the acting chief information security officer and Digital Solutions vice president direct the acting manager, Corporate Information Security Office, to:

1. Update the Mass Data Compromise Response Plan to include an external cyber intrusion focus, a security clearance requirement, critical assets, comprehensive workflow processes, incident checklists, external communication protocols, and Postal Service Handbook AS-805, *Information Security*, policy requirements that are not part of the plan.

2. Annually test the Mass Data Compromise Response Plan in accordance with industry best practices.

Management's Comments

Management generally agreed with the findings and recommendations in the report. See Appendix B for management's comments, in their entirety.

Regarding recommendation 1, management will update the MDCRP as recommended except for the external threat focus. Management disagreed with the statement that the MDCRP focused on internal threats and maintains that it was developed for both internal and external threats. Management plans to update the MDCRP by March 31, 2016.

Regarding recommendation 2, management stated that they conducted a test of the MDCRP on October 14, 2015, and will continue to test the MDCRP annually. Management requested that this recommendation be closed upon issuance of the final report.

Evaluation of Management's Comments

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

Regarding recommendation 1, the OIG found that at the time of the 2014 cyber intrusion, the MDCRP did not align with Handbook AS-805 or industry best practices because it focused on internal employee threats rather than external sophisticated attacks. The OIG will continue to monitor future updates to the MDCRP to ensure the Postal Service addresses external attacks.

Regarding recommendation 2, management will need to provide documentation related to the October 14, 2015, MDCRP testing and results before the recommendation can be closed.

The 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

Background

Cyber intrusion response is an important part of an IT program. Cybersecurity attacks have become more numerous, diverse, damaging, and disruptive with new types of incidents emerging frequently. While mitigating factors based on the results of risk assessments can lower the number of incidents, not all incidents can be prevented. Compounding this problem, preventable measures are not entirely effective against some types of attacks. Attacks such as phishing emails can use social engineering tactics to trick individuals into disclosing sensitive information or performing certain actions, such as downloading and executing malicious files. A response capability is necessary in order to rapidly detect and minimize loss, minimize the impact of the exploited weaknesses, and restore IT services.

Performing incident response effectively is a complex undertaking that requires substantial planning and resources. Organizations can reduce the impact of a cyber intrusion by having an incident response plan. The plan should establish clear procedures for prioritizing the handling of incidents; and effective methods of collecting, analyzing, and reporting data. Furthermore, it is vital that the plan address relationships and establish suitable means of communication with other internal groups, such as Human Resources and Legal; and with external groups, such as other incident response teams and law enforcement.

The U.S. Postal Inspection Service originally developed the MDCRP and in 2010 transferred the plan to CISO, which is responsible for updating and maintaining it.

Objective, Scope, and Methodology

Our objective was to assess the sufficiency and implementation of the Postal Service's MDCRP. To accomplish our objective we:

- Researched best practices for mass data compromise response plans from organizations that would create an effective model for the Postal Service. We used information from sources such as Gartner, the Department of Justice, the Carnegie-Mellon Software Engineering Institute, and the SANS Institute.
- Compared the MDCRP to best practices and identified gaps.
- Interviewed key Postal Service personnel to document the use and effectiveness of and adherence to the MDCRP for the 2014 cyber intrusion.
- Reviewed remediation project plans, daily situation reports, After Action Reports, DARs, certification and accreditation documentation for affected systems and applications, and other relevant documentation.

We did not evaluate incidents unrelated to the 2014 cyber intrusion response or the events that caused the cyber intrusion. In addition, we did not analyze the organizational structure, training programs, or low-level incident response plans.

We conducted this performance audit from February 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 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 October 28, 2015, and included their comments where appropriate. We did not assess the reliability of any computer-generated data for the purposes of this report.

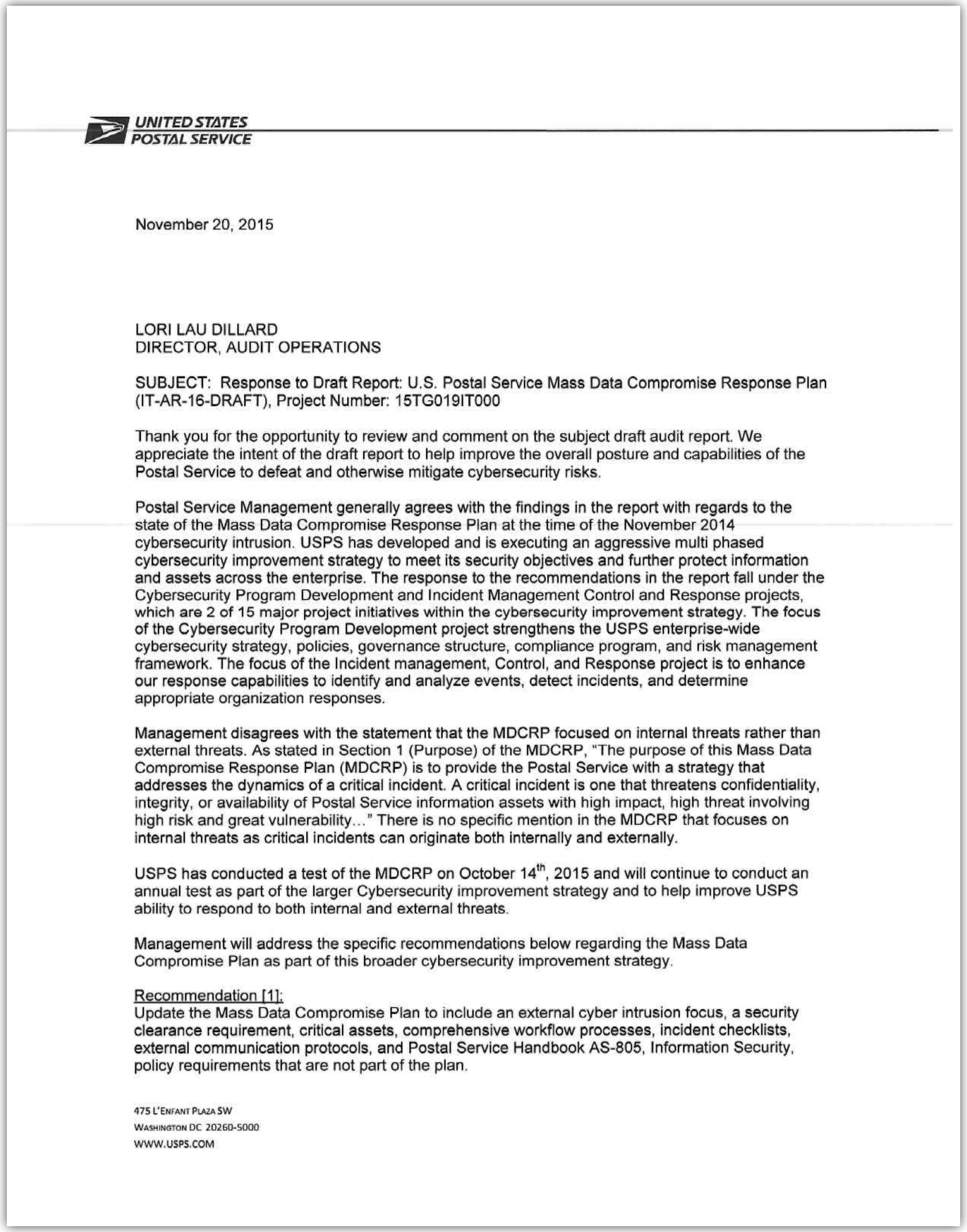
Highlights
Table of Contents
Findings
Recommendations
Appendices

Prior Audit Coverage

The OIG previously issued two reports on activities related to data backup and recovery as well as disaster recovery planning. In these reports, we provided relevant information and recommendations concerning data backups, impact assessments, and disaster recovery plan testing. The report titles and dates are in the table below.

Report Title	Report Number	Final Report Date	Monetary Impact (in millions)
Backup and Recovery of Essential Data	IT-MA-14-001	8/20/2014	None
Report Results: Our report determined that the Postal Service did not ensure that it stored all database backups on separate hardware. The Computer Incident Response Team database was lost due to a hardware failure and the data were not recovered due to the absence of a backup on a separate piece of hardware. As a result, this database was not available to help employees perform historical analyses and the Postal Service could not comply with security policy. We recommended expanding existing procedures in Handbook AS-805 to prohibit the practice of using the same hardware to maintain and backup noncritical information resources and issuing a reminder that data backups be maintained in an appropriate location to reduce potential loss, damage, or misuse of essential data. Management agreed with the findings and recommendations in the report.			
Engineering Systems and Network Operations Disaster Recovery Plan	IT-AR-13-007	9/24/2013	None
Report Results: Our report determined that Engineering Systems and Network Operations management did not establish or periodically test a disaster recovery plan. In addition, an outdated Continuity of Operations Plan listed alternative sites in case of a disaster; however, no plan exists describing how those sites would become operational in a disaster. Further, business or infrastructure impact assessments were not completed or updated for 57 of the 71 supported applications. We recommended management create and test a disaster recovery plan at an alternative site that is a sufficient distance away that it will not be affected by the same disaster and complete impact assessments for the supported applications. Management agreed with our findings and recommendations.			

Appendix B: Management's Comments



UNITED STATES
POSTAL SERVICE

November 20, 2015

LORI LAU DILLARD
DIRECTOR, AUDIT OPERATIONS

SUBJECT: Response to Draft Report: U.S. Postal Service Mass Data Compromise Response Plan (IT-AR-16-DRAFT), Project Number: 15TG019IT000

Thank you for the opportunity to review and comment on the subject draft audit report. We appreciate 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.

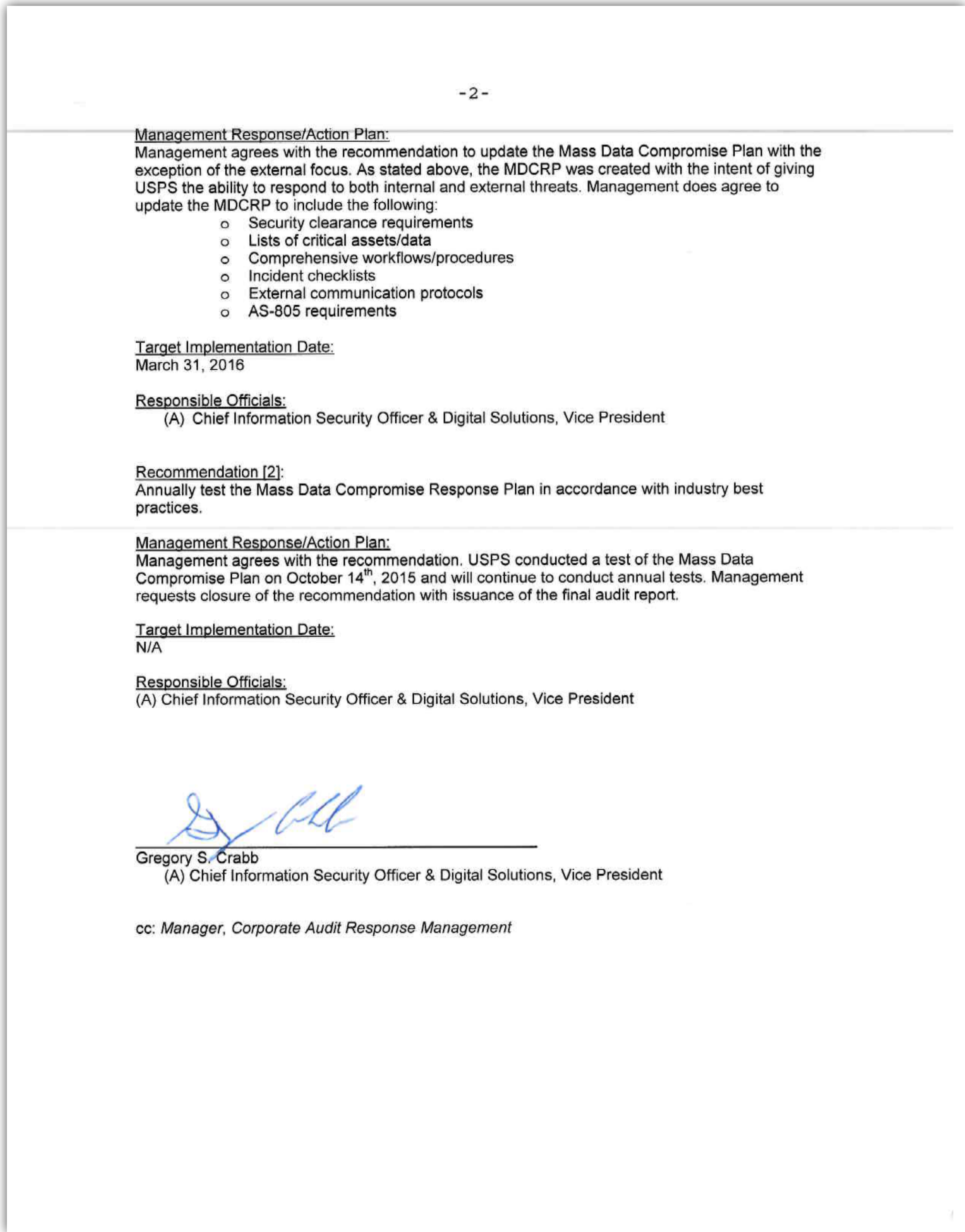
Postal Service Management generally agrees with the findings in the report with regards to the state of the Mass Data Compromise Response Plan at the time of the November 2014 cybersecurity intrusion. USPS has developed and is executing an aggressive multi phased cybersecurity improvement strategy to meet its security objectives and further protect information and assets across the enterprise. The response to the recommendations in the report fall under the Cybersecurity Program Development and Incident Management Control and Response projects, which are 2 of 15 major project initiatives within the cybersecurity improvement strategy. The focus of the Cybersecurity Program Development project strengthens the USPS enterprise-wide cybersecurity strategy, policies, governance structure, compliance program, and risk management framework. The focus of the Incident management, Control, and Response project is to enhance our response capabilities to identify and analyze events, detect incidents, and determine appropriate organization responses.

Management disagrees with the statement that the MDCRP focused on internal threats rather than external threats. As stated in Section 1 (Purpose) of the MDCRP, "The purpose of this Mass Data Compromise Response Plan (MDCRP) is to provide the Postal Service with a strategy that addresses the dynamics of a critical incident. A critical incident is one that threatens confidentiality, integrity, or availability of Postal Service information assets with high impact, high threat involving high risk and great vulnerability..." There is no specific mention in the MDCRP that focuses on internal threats as critical incidents can originate both internally and externally.

USPS has conducted a test of the MDCRP on October 14th, 2015 and will continue to conduct an annual test as part of the larger Cybersecurity improvement strategy and to help improve USPS ability to respond to both internal and external threats.

Management will address the specific recommendations below regarding the Mass Data Compromise Plan as part of this broader cybersecurity improvement strategy.

Recommendation [1]:
Update the Mass Data Compromise Plan to include an external cyber intrusion focus, a security clearance requirement, critical assets, comprehensive workflow processes, incident checklists, external communication protocols, and Postal Service Handbook AS-805, Information Security, policy requirements that are not part of the plan.



Management Response/Action Plan:
Management agrees with the recommendation to update the Mass Data Compromise Plan with the exception of the external focus. As stated above, the MDCRP was created with the intent of giving USPS the ability to respond to both internal and external threats. Management does agree to update the MDCRP to include the following:

- o Security clearance requirements
- o Lists of critical assets/data
- o Comprehensive workflows/procedures
- o Incident checklists
- o External communication protocols
- o AS-805 requirements

Target Implementation Date:
March 31, 2016

Responsible Officials:
(A) Chief Information Security Officer & Digital Solutions, Vice President

Recommendation [2]:
Annually test the Mass Data Compromise Response Plan in accordance with industry best practices.

Management Response/Action Plan:
Management agrees with the recommendation. USPS conducted a test of the Mass Data Compromise Plan on October 14th, 2015 and will continue to conduct annual tests. Management requests closure of the recommendation with issuance of the final audit report.

Target Implementation Date:
N/A

Responsible Officials:
(A) Chief Information Security Officer & Digital Solutions, Vice President

Gregory S. Crabb
(A) Chief Information Security Officer & Digital Solutions, Vice President

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