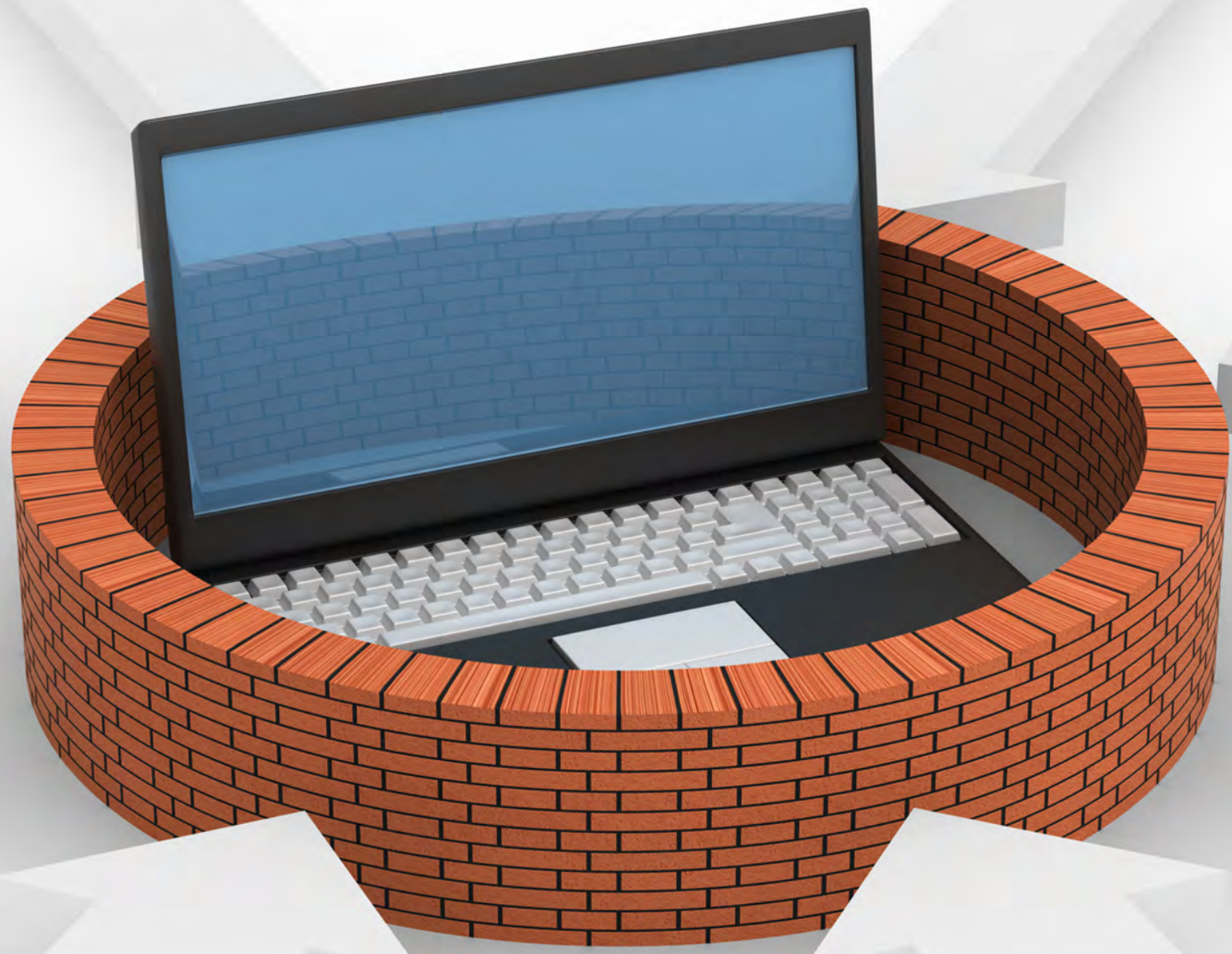
OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

# Firewall Security Review



## Audit Report

**Report Number**
**IT-AR-16-005**

**January 26, 2016**

OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

# Highlights

***Postal Service firewalls are [redacted] at all facilities and are not properly managed and functioning to safeguard mail processing operations according to Postal Service standards and industry best practices.***

Firewall Security Review
Report Number IT-AR-16-005

## Background

U.S. Postal Service mail processing equipment and mail handling equipment (MPE/MHE) includes computer systems and networks that manage, monitor, and control mail processing functions. There are about 74 types of MPE/MHE totaling more than 8,500 pieces of equipment used to sort about 155 billion mailpieces annually.

To secure its mail processing systems and control access to the MPE/MHE environment, the Postal Service relies on 285 firewalls to control the flow of network traffic. Therefore, firewall policies that effectively address security risks are critical to protecting the Postal Service network.

Our objective was to determine whether network firewalls are in place, properly managed, and functioning to safeguard Postal Service mail processing operations according to Postal Service standards and industry best practices.

## What the OIG Found

Postal Service firewalls are [redacted] at all facilities and are not properly managed and functioning to safeguard mail processing operations according to Postal Service standards and industry best practices. We identified 67 out of 352 mail processing facilities that did not [redacted] their MPE/MHE as required. Firewall administrators also did not apply six of the nine critical security controls required for any of the 30 firewalls we sampled.

In addition, firewall administrators did not manage firewall rules effectively or remove duplicate firewall rules. For the 30 firewalls in our sample, we reviewed 504,528 rules and identified [redacted] We also identified 69,258 (14 percent) rules that [redacted], and 31,754 (6 percent) were duplicate rules.

Further, we found the Postal Service does not always document and approve MPE/MHE firewall rule changes. During our audit, the Corporate Information Security Office updated the policy to include MPE/MHE rule changes in the Network Connectivity Review Board's approval process; therefore, we are not issuing a recommendation on this issue.

Finally, we determined that firewall administrators did not review and update firewall security standards annually as required.

Firewalls were [redacted] at some facilities because firewall administrators and system analysts decided to [redacted] due to budget constraints. However, management did not perform a risk assessment to determine the associated impact. In addition, Information Technology

# OFFICE OF INSPECTOR GENERAL
## UNITED STATES POSTAL SERVICE

firewall administrators and Engineering systems analysts focused on supporting system deployment as opposed to implementing critical security controls and managing firewall rules.

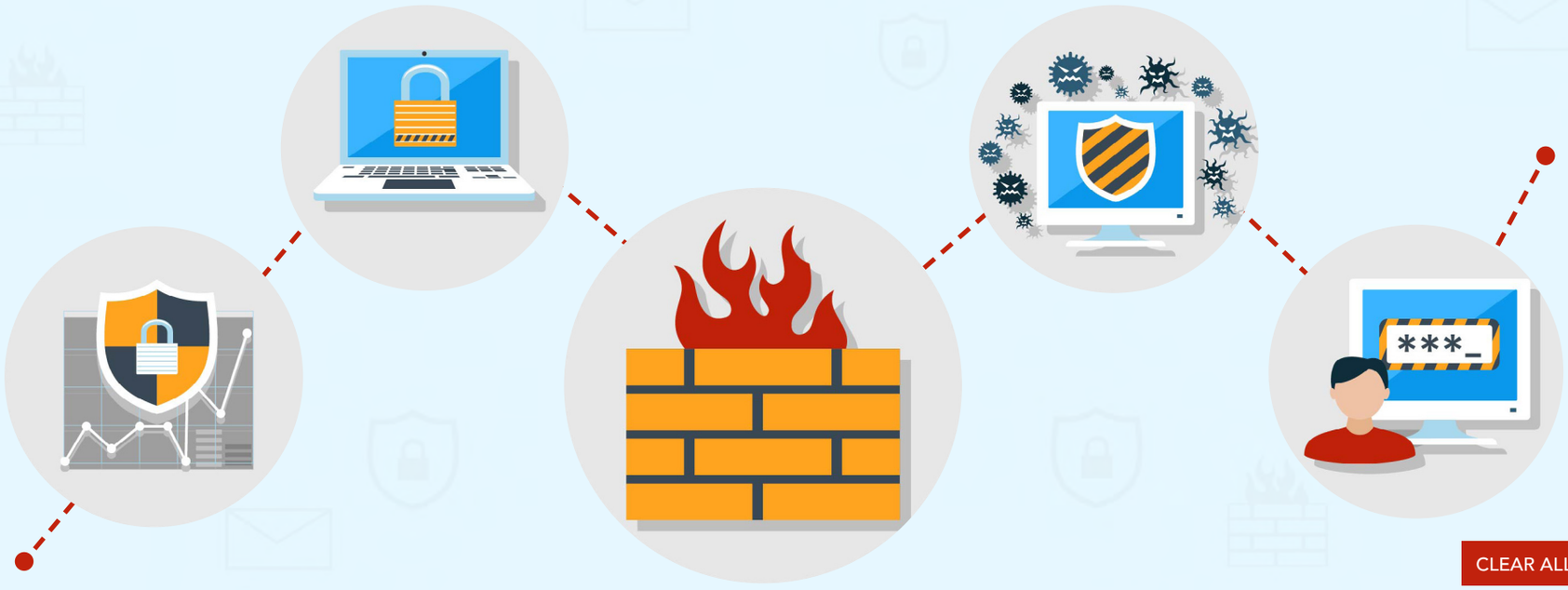
Facilities [redacted], along with improperly configured, outdated, or nonexistent firewall security controls, significantly decrease the Postal Service's network security. This increases the risk of unauthorized access to data and disruption of critical mail processing operations.

## What the OIG Recommended

We recommended administrators and analysts [redacted] at all mail processing facilities. In addition, we recommended firewall administrators regularly review and update current firewall configuration settings and implement all security controls in the hardening standards. Finally, we recommended administrators and analysts review firewall rules every 6 months and review and update firewall security standards annually in accordance with policy.

## OIG Recommendations:

*Click images to reveal a summary of OIG recommendations.*



# Transmittal Letter

OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

January 26, 2016

**MEMORANDUM FOR:** BRIAN W. CARNELL
ACTING VICE PRESIDENT, INFORMATION TECHNOLOGY

MICHAEL J. AMATO
VICE PRESIDENT, ENGINEERING SYSTEMS

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

E-Signed by Kimberly Benoit
VERIFY authenticity with eSign Desktop

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

**SUBJECT:** Audit Report – Firewall Security Review
(Report Number IT-AR-16-005)

This report presents the results of our audit of the Postal Service's Firewall Security Review (Project Number 15TG036IT000).

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 703-248-2100.

Attachment

cc: Corporate Audit and Response Management

# Table of Contents

# Findings

***Firewall administrators did not [redacted] at 67 out of 352 mail processing facilities, as required by Postal Service policy.***

## Introduction

This report presents the results of our self-initiated audit of the U.S. Postal Service's firewall security review (Project Number 15TG036IT000). Our objective was to determine whether network firewalls are in place, properly managed, and functioning to safeguard mail processing operations according to Postal Service standards and industry best practices. See Appendix A for additional information about this audit.

The Postal Service has one of the world's largest information technology (IT) networks to store, transmit, and process sensitive employee, customer, financial, law enforcement, and injury compensation data. Therefore, it is vital that the Postal Service secures sensitive information to allow for uninterrupted mail processing and network operations, and maintain the trust of the American public.

Postal Service mail processing equipment and mail handling equipment[1] (MPE/MHE) includes computer systems and networks that manage, monitor, and control mail processing functions. In addition, these systems collect workload statistics and transmit data between the MPE/MHE and Postal Service information systems. There are about 74 different types of MPE/MHE totaling more than 8,500 pieces of equipment used to sort about 155 billion mailpieces annually. To secure its mail processing systems, the Postal Service relies on 285 firewalls[2] to control the flow of network traffic. These firewalls help control access to MPE/MHE systems and resources; therefore, firewall policies that effectively address security risks are critical to protecting the Postal Service and its network.

## Summary

Postal Service firewalls are [redacted] at all facilities and are not properly managed and functioning to safeguard mail processing operations according to Postal Service standards and industry best practices. Specifically, we identified [redacted] mail processing facilities that [redacted] to protect their MPE/MHE. In addition, for the 30 firewalls we sampled,[3] firewall administrators did not apply six of the nine critical security controls as required by the Postal Service's security standards.

Further, firewall administrators did not manage firewall rules effectively and did not remove duplicate firewall rules. For the 30 firewalls in our sample, we reviewed 504,528 rules and identified four rules that allowed [redacted] to flow [redacted] through two firewalls. We also identified 69,258 (14 percent) rules that allowed network traffic from [redacted], and 31,754 (6 percent) duplicate rules. We also found that the Postal Service does not always document and review MPE/MHE firewall rule changes and firewall administrators did not review and update firewall security standards in accordance with Postal Service policy.

These issues exist because firewall administrators and system analysts decided to [redacted] due to budget constraints. In addition, IT firewall administrators and Engineering Systems analysts focused on supporting system deployment as opposed to implementing security controls and managing firewall rules. Further, the telecommunications infrastructure[4] at mail processing facilities is not equipped to handle [redacted]. Facilities [redacted], along with improperly configured, outdated, or nonexistent firewall security controls, significantly

1 Examples of mail processing and handling equipment include the Automated Flat Sorting Machine (AFSM), Delivery Barcode Sorter (DBSC), and National Directory Support System (NDSS).
2 A network security device designed to control incoming and outgoing network traffic based on predetermined security rules.
3 See Table 1 for a listing of the 30 firewalls we sampled.
4 Telecommunication infrastructure refers to the transmission or exchange of information over significant distances by electronic means.

decrease the Postal Service's network security. This increases the risk of unauthorized access to data and disruption of critical mail processing operations.

## Mail Processing Facilities Without Firewalls

Firewall administrators did not [redacted] at 67 out of 352 mail processing facilities, as required by Postal Service policy.[5] Due to budget constraints, firewall administrators and system analysts decided to place [redacted]; however, they did not perform a risk assessment to determine and document the impact of [redacted] Without [redacted], the Postal Service does not have a reliable and secure network and is at risk of unauthorized access to data and disruption of critical mail processing operations.

## Firewall Configuration Review

Firewall administrators did not apply six of nine critical security controls[6] across the 30 firewalls in our sample. Specifically, we found that firewall administrators did not configure firewalls to:

- [redacted]

- Use [redacted][8] The firewalls in our sample used [redacted] Postal Service hardening standards[9] require the use of [redacted] which uses an improved and stronger process for encryption and includes a secure file transfer protocol that adds more security to minimize vulnerabilities.

- Update the time upon start-up. Postal Service hardening standards[10] require the Network Time Protocol (NTP)[11] to be configured to update firewall time upon start-up. Time synchronization protocols are important during forensic analysis following a network intrusion.

- Enable session timeout for [redacted]. Postal Service hardening standards[12] require session timeout of 60 seconds or less for [redacted], which limits the potential for misuse of unattended sessions.

- Enforce password complexity or minimum length requirements. Current firewall configurations require passwords to have a [redacted], but Postal Service policy[13] states passwords must consist of at least 15 characters and include a combination of characters and numbers, which limits the potential for a password compromise.

- Use a current operating systems version. The firewalls are currently running [redacted]. As of [redacted], the vendor no longer provides security updates or support for this version. Attackers could exploit known operating system flaws to compromise the network.

---

5 Handbook AS-805, Section 11-5.2, [redacted].
6 Controls identified and approved in Postal Service policy and security hardening standards. See Table 2 for a list of security controls we reviewed.
7 *Security Hardening Standards for* [redacted], Section 5.1, General Audit Logging Requirements, dated [redacted].
8 A [redacted] for secure access to remote computers.
9 *Security Hardening Standards for* [redacted], Section 4.5.1, [redacted].
10 *Security Hardening Standards for* [redacted], Section 4.12.1 Use NTP Boot-Server.
11 A protocol that synchronizes computer clock times over a network. Network security logs and event analysis depend on accurate time synchronization.
12 *Security Hardening Standards for* [redacted], Section 4.2.5, Configure Idle Timeout for All Login Classes.
13 Handbook AS-805, *Information Security*, Section 9-6.1.1, Password Selection Requirements, dated May 2015.

These issues occurred because IT administrators and Engineering Systems analysts focused on supporting system deployment as opposed to implementing required configurations and restricting network traffic. In addition, the manager, Perimeter Security Services, stated that the amount of system log data generated by the firewalls caused network performance and availability issues.

Without adequate and effective security controls, the Postal Service cannot effectively identify and respond to security events that could result in unauthorized disclosure of sensitive data and disruption of mail processing operations. We determined about $237 million of revenue was processed at 15[14] of the 30 facilities in our sample during Quarter (Q) 3, FY 2015.

## Firewall Rules Management

We determined firewall administrators did not identify and remove overly permissive[15] and duplicate firewall rules to control network traffic, prevent unauthorized access to data and avoid disrupting mail processing operations. According to Postal Service hardening standards[16] and industry best practices,[17] firewall rules should allow only necessary network traffic. In addition, firewall rules should be as specific as possible to allow the types[18] of traffic that are required to support mail processing systems and applications. For the 30 firewalls in our sample, we reviewed 504,528 rules. During our review:

- [redacted]
- We identified 51,656 (10 percent) firewall rules that permitted network traffic [redacted]; 13,852 (3 percent) firewalls rules that permitted network traffic [redacted]; and 3,750 (1 percent) firewall rules that permitted communication to [redacted] in the administrative and mail processing infrastructure (MPI) networks.
- We identified 30,196 (6 percent) rules that allowed unencrypted data to flow across the network and 721 (less than 1 percent) rules that allowed the use of [redacted].
- We identified 31,754 (6 percent) duplicated rules that could degrade firewall performance and limit the firewall's ability to respond to connection requests and process legitimate network traffic. An excessive number of duplicate rules also make it more difficult to manage all of the rules in an efficient manner.

Overly permissive or duplicate firewall rules existed because firewall administrators did not review rules semiannually according to policy.[21] In addition, administrators and analysts did not identify critical elements for developing secure rules. These elements include source IPs, destination IPs, and applications. Identifying these elements would allow administrators and analysts to customize the rule sets to secure the network environment without any business impact. In addition, contractors developed the

---

14 For this analysis we only calculated total revenue associated with competitive mail (Flats and Parcels) that was processed through Postal Service plants. This number only includes 15 facilities from our sample that were part of the Postal Service's statistical sample for Revenue Pieces Weights-Orgin Destination Information System during Q3, FY 2015.
15 [redacted].
16 *Security Hardening Standards for* [redacted], Section 4.14, Services.
17 National Institute of Standards and Technology (NIST) Special Publication 800-41, [redacted] dated September 2009.
18 Types of traffic include protocols, services, and source and destination IP addresses.
19 [redacted]
20 [redacted].
21 Handbook AS-805, Section 11.5-2, [redacted].

***Firewall administrators did not review and update firewall security standards in accordance with Postal Service policy and industry best practices. Specifically, firewall administrators have not reviewed and updated security standards since [redacted]***

current rule sets based on legacy rules migrated from the previous firewall environment, which used a different firewall product. Obsolete and misconfigured firewall rules may limit firewall performance, which curtails the firewall's ability to respond to network connection requests and process legitimate network traffic.

We also found that the Postal Service did not document and approve 63,764 of 85,027 (75 percent) MPE/MHE firewall rule changes prior to implementation because Postal Service policy did not designate the responsible authority for approving the changes. Without an established change management process, the Postal Service may implement firewall rule changes that disrupt critical mail processing operations or conflict with other rules. During our audit, the manager, Corporate Information Security, updated Handbook AS-805 to state that MPE/MHE firewall rule changes require Network Connectivity Review Board (NCRB) approval. Therefore, we will not make a recommendation regarding this issue.

## Firewall Hardening Standards

Firewall administrators did not review and update firewall security standards in accordance with Postal Service policy[22] and industry best practices. Specifically, firewall administrators have not reviewed and updated security standards since [redacted] because they believed their initial configurations were reliable and needed no changes. However, they did not perform a review to ensure that the configurations included the latest updates to secure the environment against new potential threats and vulnerabilities. Lack of and outdated security controls increase the risk of unauthorized access to data and disruption of critical mail processing operations.

22 Handbook AS-805, Section 11-5.2, [redacted]

# Recommendations

***We recommend management perform a risk assessment for all mail processing facilities [redacted] to ensure that they are protected as appropriate or document acceptance of the risk; and review and update the [redacted] firewall security standards annually in accordance with Handbook AS-805, Information Security.***

We recommend the acting vice president, Information Technology, and the vice president, Engineering Systems, direct the managers, Enterprise Asset Infrastructure and Engineering Software Management, to:

1. Perform a risk assessment for all mail processing facilities [redacted] to ensure that they are protected as appropriate or document acceptance of the risk.

We recommend the acting vice president, Information Technology, direct the manager, Enterprise Asset Infrastructure, to:

2. Configure firewalls to enforce [redacted], proper encryption, network time protocol, session timeouts, and password complexity; and update the firewall operating system.

3. Update the telecommunication infrastructure to support firewall [redacted] capabilities at all mail processing facilities.

We recommend the acting vice president, Information Technology, and the vice president, Engineering Systems, direct the managers, Enterprise Asset Infrastructure and Engineering Software Management, to:

4. Review current firewall rules and remove those that are overly permissive or duplicative and; review firewall rules every 6 months according to Handbook AS-805, *Information Security,* and document the results of the review.

We recommend the acting vice president, Information Technology, and the acting Chief Information Security Officer and vice president Digital Solutions, direct the managers, Enterprise Asset Infrastructure and Corporate Information Security, to:

5. Review and update the [redacted] firewall security standards annually in accordance with Handbook AS-805, *Information Security*.

## Management's Comments

Management agreed with recommendations 1 through 4 and disagreed with recommendation 5 and the $237 million in potential revenue at risk. Management also stated that they agreed with all of the findings in the report. Management stated that their priorities have always been improving the overall security posture and have efforts underway to enhance firewall and network security. See Appendix B for management's comments in their entirety.

Regarding recommendation 1, management stated that funding is in place and efforts are underway to upgrade existing firewalls and install new firewall technology at all mail processing facilities. The target implementation date is December 31, 2017.

Regarding recommendation 2, management will configure firewalls to ensure proper encryption, network time protocol, session timeouts, and password complexity; and update the firewall operating system. In addition, management will work with the Enterprise Splunk team to determine the appropriate level of logging activity for the firewalls and configure them accordingly. The target implementation date is September 30, 2017.

Regarding recommendation 3, management will work with the Enterprise Splunk team to determine the appropriate level of logging activity for firewalls and configure them accordingly. The target implementation date is September 30, 2016.

Regarding recommendation 4, management will review existing firewall rules and remove any that are duplicative or which grant inappropriate access. Additionally, upon completion of the initial clean-up effort, management will perform a semiannual review of firewall rules in accordance with policy. The target implementation date is September 30, 2017.

Regarding recommendation 5, management disagreed with the recommendation and stated that they have begun a large-scale network upgrade that includes replacing all existing [redacted] devices with [redacted] devices and installing this technology at all mail processing facilities. Management will replace the [redacted] firewall security standards with [redacted] security standards, which they will review and update annually. The target implementation date is September 30, 2017.

Regarding the $237 million in potential revenue at risk, management disagreed with our calculation and stated that the likelihood of a potential malicious actor exploiting firewall vulnerabilities and simultaneously penetrating mail processing facilities and disrupting mail processing is extremely remote. Management also stated that they have monitoring practices in place to identify an attack within minutes and both manual and automated contingency plans in place to ensure mail processing operations continue in the event of a disruption to the network. Management calculated an impact of $175,393.

## Evaluation of Management's Comments

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

Regarding recommendation 5, we agree that a large-scale network upgrade that includes replacing all existing [redacted] devices with [redacted] devices and replacing [redacted] firewall security standards with [redacted] security standards should resolve the issue identified in the report. However, based on the target implementation date provided, management should continue updating the [redacted] security standards to support the firewalls currently in place. This recommendation will remain open until management provides documentation supporting the network upgrade.

Management stated that they disagreed with the calculated $237 million in potential revenue at risk. We based our analysis on the amount of revenue exposed to the risks we identified in our report and agree that this is not the amount of revenue that would be lost during a single incident. We clarified in the report that $237 million is the amount of competitive mail revenue processed at 15 of the 30 facilities in our sample during Q3, FY 2015.

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

## Background

Cyber threats have become more sophisticated and have increased significantly over the past decade. Hackers can cause damage on a large scale. In order to protect information resources and mail processing operations from unauthorized intrusion and disruption, the Postal Service established standards for hardening information resources. Hardening is a security activity that ensures all unnecessary services are disabled, security-related patches are applied to operating systems and applications, and security-related configuration settings are in place and set up correctly. The primary goal is to support the creation of a strong security infrastructure to protect the Postal Service's electronic-business applications, data, and critical mail processing operations.

The Postal Service relies on firewalls to protect information resources and secure its mail processing systems. Firewalls are security devices that control the flow of network traffic and check against approved policies to either allow or block traffic based on those policies. Policies should be based on the direction that the traffic moves across the network. This feature allows firewalls to restrict connections to and from the internal networks, which prevents unauthorized access to systems and resources. The Postal Service uses two brands of firewalls to control network traffic – [redacted] firewalls are used on the IT network for perimeter protection and [redacted] firewalls are used in the MPI environment for internal network protection.

## Objective, Scope, and Methodology

Our objective was to determine whether network firewalls are in place, properly managed, and functioning to safeguard mail processing operations according to Postal Service standards and industry best practices. Our audit scope covered approved firewall configuration baselines, security standards, and policies used to support mail processing operations at Postal Service facilities. We conducted our audit work at Postal Service Headquarters; Engineering Systems Headquarters in Merrifield, VA; and the Information Technology Service Center in Raleigh, NC.

To accomplish our objective we:

- Reviewed policies and standards related to firewalls and interviewed IT, Corporate Information Security, and Engineering Systems personnel to identify facilities without firewalls.
- Interviewed IT, Corporate Information Security, and Engineering Systems personnel to obtain an understanding of network security controls for the MPE/MHE environment.
- Obtained the firewall inventory and selected a random sample of 30 firewalls to review and assess the sufficiency of their configurations against the approved Postal Service firewall security standards and controls.
- Compared the Postal Service firewall hardening standards to industry best practices and documented discrepancies.
- Interviewed Engineering Systems and IT personnel to identify and document MPE/MHE applications and servers.
- Reviewed firewall configurations, rules sets, and policies to determine whether appropriate controls were in place.

Table 1 identifies the 30 facilities we randomly sampled. Each facility has one firewall identified by type of mail processing facility and location.

**Table 1. MPE/MHE Firewalls Reviewed**

| Mail Processing Facility | City | State |
|---|---|---|
| [redacted] | | |

Source: Postal Service Telecom Services team and OIG analysis.

Table 2 identifies the nine security controls assessed for the 30 firewalls in our sample.

**Table 2. [redacted] Firewall Security Controls**

| Number of Security Controls | Security Control | Compliant With Security Standards |
|---|---|---|
| 1 | [redacted] | No |
| 2 | [redacted] | No |
| 3 | [redacted] | No |
| 4 | [redacted] | Yes |
| 5 | [redacted] | Yes |
| 6 | [redacted] | Yes |
| 7 | [redacted] | No |
| 8 | [redacted] | No |
| 9 | [redacted] | No |

Source: Postal Service [redacted] Security Standards and OIG analysis.

We conducted this performance audit from July 2015 through January 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 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 December 18 and December 22, 2015, and included their comments where appropriate.

We assessed the reliability of firewall configurations and rules data by reviewing information stored in the [redacted] Network Management and the NCRB change management systems. In addition, we interviewed agency officials knowledgeable about the data and process and tested required security controls. We determined that the data were sufficiently reliable for the purposes of this report.

## Prior Audit Coverage

We did not identify any prior audits or reviews related to the objective of this audit.

---

23 [redacted]

24 Console logins left unattended by firewall administrators can compromise sensitive network information or allow accidental or intentional configuration changes by unauthorized personnel.

# Appendix B: Management's Comments

UNITED STATES POSTAL SERVICE

LORI LAU DILLARD
DIRECTOR, AUDIT OPERATIONS

SUBJECT: Response to Draft Report: Firewall Security Review (IT-AR-16-DRAFT), Project Number 15TG036IT000

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 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 protect information and assets across the enterprise. As part of this strategy, USPS management has already approved funding and initiated an effort to enhance firewall and network security that addresses many of the findings identified in this report. This effort includes installing new firewall technology at all mail processing facilities. The USPS will work diligently to remediate all the firewall improvements. The dates below represent the estimated time it will take to complete the recommendations.

Recommendation [1]:
Perform a risk assessment for all mail processing facilities without firewalls and install technology to ensure that they are protected as appropriate or document acceptance of the risk.

Management Response/Action Plan:
Management agrees with the recommendation. Funding is in place and efforts are already underway to upgrade existing firewalls and install new firewall technology at all mail processing facilities by 2017.

Target Implementation Date(no later than):
December 31, 2017

Responsible Official:
Manager, Enterprise Access Infrastructure, Information Technology
Manager, Engineering Software Management, Engineering Systems

Recommendation [2]:
Configure firewalls to enforce [redacted] proper encryption, network time protocol, session timeouts, and password complexity; and update the firewall operating system.

Management Response/Action Plan:
Management agrees with the intent of the recommendation. Management will work with the Enterprise Splunk team to determine the appropriate level of [redacted] activity for firewalls and configure them accordingly. Additionally, management will configure firewalls to ensure proper encryption, network time protocol, session timeouts, and password complexity; and update the firewall operating system.

475 L'Enfant Plaza SW
Washington DC 20260-5000
www.usps.com

Target Implementation Date(no later than):
September 30, 2017

Responsible Official:
Manager, Enterprise Access Infrastructure, Information Technology

Recommendation [3]:
Update the telecommunication infrastructure to support firewall [redacted] capabilities at all mail processing facilities.

Management Response/Action Plan:
Management agrees with the intent of the recommendation. Management will work with the Enterprise Splunk team to determine the appropriate level of [redacted] activity for firewalls and configure them accordingly.

Target Implementation Date(no later than):
September 30, 2016

Responsible Official:
Manager, Enterprise Access Infrastructure, Information Technology

Recommendation [4]:
Review current firewall rules and remove those that are permissive or duplicative and; review firewall rules every 6 months according to Handbook AS-805, *Information Security*, and document the results of the review.

Management Response/Action Plan:
Management agrees with the intent of this recommendation. Management will begin the substantial effort of reviewing all existing firewall rules and will remove any that are duplicative or which grant inappropriate access. Once this initial firewall clean-up effort is completed, management agrees to perform a semiannual review of firewall rules in accordance with policy.

Target Implementation Date(no later than):
September 30, 2017

Responsible Official:
Manager, Enterprise Access Infrastructure, Information Technology
Manager, Engineering Software Management, Engineering Systems

Recommendation [5]:
Review and update the [redacted] firewall security standards annually in accordance with Handbook AS-805, *Information Security*.

Management Response/Action Plan:
Management disagrees with the recommendation to review and update the [redacted] firewall security standards. Management has begun a large network upgrade effort that includes replacing all of the existing [redacted] devices with [redacted] devices and installing this new firewall technology at all mail processing facilities. As part of this effort, the existing [redacted] firewall security standards will be replaced with the latest [redacted] security standards and will be reviewed and updated annually.

Target Implementation Date(no later than):
September 30, 2017

Responsible Official:
Manager, Enterprise Access Infrastructure, Information Technology
Manager, Corporate Information Security Office, CISO

Michael J. Amato
Vice President, Engineering Systems

1/11/2018

Brian W. Carnell
(A) Vice President, Information Technology

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

cc: *Manager, Corporate Audit Response Management*

[redacted]

Michael J. Amato
Vice President, Engineering Systems

1/11/2016
Brian W. Carnell
(A) Vice President, Information Technology

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.
Stay informed.

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