OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

Topeka, KS, Material Distribution Center – Information Technology Logical Access Controls

Audit Report

Report Number
IT-AR-14-007

July 11, 2014

OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

Highlights

These security weaknesses could result in unauthorized access to the check printing and inventory management applications and modification of their data.

Topeka, KS, Material Distribution Center – Information Technology Logical Access Controls
Report Number IT-AR-14-007

Background

The Material Distribution Center (MDC) in Topeka, KS, provides critical and essential services to all U.S. Postal Service facilities such as parts, equipment, supplies, and print services. The MDC distributes materials to about 31,000 facilities, and it warehouses more than 26,000 items. The MDC uses an application to manage inventory, including shipment of about 112 million blank money orders to post offices around the country. It also uses a check printing application to print about 192,000 payroll checks per month.

Because of the vital services the MDC provides, it is imperative that it adhere to Postal Service policies for maintaining and securing these applications.

Our objective was to determine whether electronic safeguards for the check printing and inventory management applications were operating effectively to protect data from unauthorized modification, loss, and disclosure. Electronic safeguards include operating system updates, database configuration, [redacted] software, and web application security.

What The OIG Found

The MDC did not adequately safeguard the 14 servers that support the check printing and inventory management applications, thereby jeopardizing the security of their data. Specifically, management did not update the operating systems on any of the 14 servers or configure three database servers in accordance with security standards. In addition, the MDC did not use [redacted] software on two servers or adequately protect [redacted] server from unauthorized use. These security issues occurred because administrators were focused on other priorities, such as configuring applications for the January 2014 postage rate increase and securing the environment for credit card activity. In addition, due to an oversight, management did not ensure that security configurations were reviewed on the web application server.

What The OIG Recommended

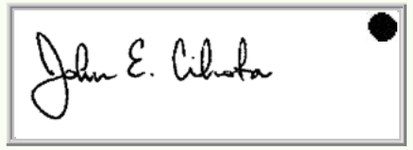
We recommended management properly configure databases, verify that the latest approved [redacted] software is enabled on operating systems, and develop a process to ensure security configurations are reviewed on all web servers. We are not making a recommendation regarding updating operating systems because management completed corrective action during the audit.

Transmittal Letter

OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

July 11, 2014

MEMORANDUM FOR: JOHN T. EDGAR
VICE PRESIDENT, INFORMATION TECHNOLOGY



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

SUBJECT: Audit Report –Topeka, KS, Material Distribution Center – Information Technology Logical Access Controls (Report Number IT-AR-14-007)

This report presents the results of our audit of the U.S. Postal Service's Topeka, KS, Material Distribution Center Information Technology Logical Access Controls (Project Number 14BG001IT000).

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

Attachment

cc: Corporate Audit and Response Management

Table of Contents

Findings

Introduction

This report presents the results of our self-initiated audit of the U.S. Postal Service's Topeka, KS, Material Distribution Center's (MDC) information technology (IT) logical access controls[1] (Project Number 14BG001IT000). Our objective was to determine whether electronic safeguards for the check printing and inventory management applications were in place and operating effectively to protect data from unauthorized modification, loss, and disclosure. Electronic safeguards include configuring databases, updating operating systems, using [redacted] software, and securing web applications. See Appendix A for additional information about this audit.

The MDC provides critical and essential services to all Postal Service facilities such as parts, equipment, supplies, and print services. The MDC distributes materials to about 31,000 facilities, warehouses more than 26,000 items, and manages inventory. In addition, the MDC annually ships about 112 million blank money orders to post offices around the country.

In 1975, the Postal Service added the Label Printing Center (LPC) to the MDC. In June 2013, it changed the LPC's name to the National Print Center (NPC) to reflect its mission of consolidating Postal Service print operations into the new center. All print functions, such as payroll checks and earning statements, are now printed at the NPC. The NPC prints about 192,000 payroll checks per month and 12 million earning statements per year.

The Infoprint Process Director (IPPD)[2] is one of the applications used to manage the printing process. Another application, the Material Distribution and Inventory Management System (MDIMS),[3] is used to manage inventory. Because of the vital services the MDC provides, it is imperative that it adhere to Postal Service policies and procedures for maintaining and securing the IPPD and MDIMS applications.

The Corporate Information Security Office provides hardening standards[4] to support the creation of a strong security infrastructure and protect Postal Service electronic business applications and sensitive customer and internal data. The primary reason for these standards is to protect electronic transactions from increasing external (non-employee) and internal (employee) threats, such as computer [redacted] and data modification. These threats can be either malicious or benign.

Logical access controls are often built into the operating system or may be part of the logic of application programs. These controls protect computer systems and data by verifying and validating authorized users, authorizing user access to computer systems and data, and restricting transactions according to the user's authorization level.

1 Electronic controls in computer systems used to prevent or detect unauthorized access such as passwords and account restrictions.
2 A database-driven print workflow system that manages all aspects of a printing process. In this case, the application manages the print environment for the NPC.
3 A real-time system used to perform material distribution, warehousing, and inventory management business functions for the Postal Service.
4 Hardening standards provide security requirements and controls for all information resources. The standards apply to all devices with connectivity to the Postal Service's computing infrastructure including, but not limited to, server hardware or devices operating server software, such as databases, operating systems, and servers.

[redacted]

Servers supporting the distribution and inventory management of money orders were not adequately safeguarded.

Conclusion

The MDC did not adequately safeguard any of the 14 servers supporting the IPPD and MDIMS applications to protect against data modification, loss, and disclosure. Specifically, management did not update the operating systems on any of the 14 servers; did not configure three database servers in accordance with security standards; did not use [redacted] software on two servers; and inadequately protected one web application server from unauthorized use. These security issues occurred because administrators were focusing on other priorities, such as configuring applications for the January 2014 postage rate increase and securing the environment for credit card activity. In addition, due to an oversight, management did not ensure security configurations were reviewed on the web application server.

These security weaknesses could result in unauthorized access to the IPPD and MDIMS applications and modification of their data. We estimated that 75,619 money orders with the potential value of about $76 million are at risk of theft annually due to inadequate security controls on all 14 servers. Effective security controls increase the probability that the Postal Service will detect and prevent a data compromise that might negatively affect the confidentiality, integrity, and availability of information resources.[6]

Patch Management[7] Compliance

Administrators[8] did not install the latest operating system software updates on any of the 14 servers that support the IPPD and MDIMS applications.[9]

Specifically:

- We identified 14 software security updates that were not installed on the two print servers supporting the IPPD application. Management decided not to install patches during the normal patch cycle[10] due to the holiday season and price rate change. During our audit, administrators installed all 14 updates on servers in subsequent patch cycles; therefore, we are not making a recommendation for this issue.

- We identified 42 software security updates that were not installed on the 12 servers supporting the MDIMS application. Management stated that they deferred installation of updates until they upgraded the servers. During our audit, administrators installed all 42 updates on servers in subsequent patch cycles; therefore, we are not making a recommendation for this issue.

See Appendix B for specific details on the update issues related to the IPPD and MDIMS servers.

---

6 All Postal Service information assets, including information systems, hardware, software, data, and applications.
7 Patch management is the process for identifying, acquiring, installing, and verifying patches for products and systems. Patches correct security and functionality problems in software and firmware.
8 IPPD and MDIMS administrators are in Eagan, MN.
[redacted]
10 The normal patch cycle for deploying [redacted] Server Security patches is [redacted]. During this period, management analyzes, tests, and applies (if appropriate) vendor-recommended patches.

Table 1 summarizes the 56 software updates the U.S. Postal Service Office of Inspector General's (OIG) automated scanning tools determined were missing from one or more of the 14 servers we tested. Table 2 summarizes the 56 updates in Table 1 by age.

Table 1. Missing Critical[11] and High-Risk[12] Updates

Application Name	Number Of Servers Affected	Operating System[1]	Third Party[2]	Database[3]	Total Unique Vulnerabilities
IPPD	2	8	6	0	14
MDIMS	12	5	23	14	42
TOTAL	**14**	**13**	**29**	**14**	**56**

Source: OIG Nessus and GFI LanGuard scanning tool results

1 A software that manages all other programs running on a computer.

2 Programs developed by companies other than the company that developed the computer's operating system.

3 Database software describes any software designed for creating databases and managing the information stored in them.

Table 2. Missing Updates By Age

Application Name	Update Age				
	0-30 days[1]	31-60 days	61-90 days	91+ days	TOTAL
IPPD	4	6	0	4	14
MDIMS	3	0	2	37	42
TOTAL	**7**	**6**	**2**	**41**	**56**

Source: OIG Nessus and GFI LanGuard scanning tool results

1 The vendor recommends that critical patches be applied immediately.

As a result, the IPPD and MDIMS applications did not have adequate safeguards in place to protect applications and data from damage or compromise. Managing updates are critical for ensuring the integrity and reliability of information resources. Untimely installation of updates could allow an attacker to run malware[13] or obtain sensitive information.

11 A rating that an IT vendor (such as Microsoft) assigns to communicate the severity of a security weakness. In this case, a critical rating means the worst scenario could occur, such as a system being hacked. The vendor recommends the customer apply the update immediately.

12 A rating that an IT vendor assigns to communicate the severity of the risk. In this case, it evaluates the level of risk associated with the security risk. The vendor recommends the customer apply the update at the earliest opportunity.

13 Malware is software programs designed to damage or perform unwanted actions to a computer system.

Inventory management servers had [redacted] disabled, [redacted]

[redacted] Database Compliance

[redacted] database administrators[14] improperly configured three of five[15] database servers supporting the MDIMS application. Specifically, we identified 15 unique security settings that were not configured in accordance with Postal Service hardening standards.[16] See Appendix C for specific details on the configuration issues related to the MDIMS application databases. Administrators did not properly configure the servers after the Postal Service revised its hardening standards in June 2013 because they had other priorities, such as configuring a secure enclave[17] to comply with Payment Card Industry Security Standards.[18] When databases are not configured correctly, a person could read and, accidentally or intentionally, change, add, or delete an order for supplies such as blank money order stock entered into MDIMS. As a result, we estimated 151,238 money orders with the potential value of about $151 million are at risk of theft over 2 years due to inadequate security controls on the 14 servers.

[redacted] Compliance

We determined that two of the 12 application servers we tested supporting the MDIMS application did not have approved and [redacted] enabled on the [redacted] operating system. See Appendix D for a summary of the security compliance settings we reviewed. This occurred because administrators decided to disable the [redacted] software on the two servers because they thought it was incompatible with MDIMS; however, the administrators did not confirm that the [redacted] software was incompatible, nor did they install [redacted] software on these servers. [redacted] During our audit administrators began running tests to re-enable [redacted] software on the two application servers.

14 [redacted] database administrators are in Raleigh, NC.
15 We performed [redacted] database scans on the three databases that were classified as production databases for MDIMS. [redacted]
16 *Security Hardening Standards for* [redacted]
17 An enclave is a network area where special protections and access controls, such as firewalls and routers, are used to secure information resources.
18 A set of requirements designed to ensure that all companies that process, store, or transmit credit card information maintain a secure environment.
19 *Security Standards for* [redacted]

Web Application Compliance

[redacted] Servers[20] supporting the MDIMS application was not adequately protected from unauthorized modification, loss, and disclosure. Specifically, we identified security weaknesses as follows:

- [redacted]
- [redacted]
- [redacted]

These vulnerabilities existed because management did not ensure a security code review[24] was performed and documented on MDIMS. As a result, an unauthorized person could obtain sensitive data and compromise IT security.

20 Provides the environment to run web-enabled applications. This development server was replicated from the production server specifically for our testing because of the possibility of corrupting the production environment with script injection and parameter manipulation.

[redacted]

24 A security code review is an analysis of the source code and documentation to verify compliance with software design documents and programming standards and the absence of malicious code.

Recommendations

We recommend management properly configure databases; verify the latest and approved [redacted] is enabled on operating systems; and develop a process to ensure security configurations are reviewed on all web servers.

We recommend the vice president, Information Technology, direct the manager, Solutions Development and Support, to:

1. Configure and update all database servers that support the Material Distribution and Inventory Management System application.

2. Verify the latest approved [redacted] software is enabled on all servers supporting the Material Distribution and Inventory Management System application.

3. Review security codes on all web servers that support the Material Distribution and Inventory Management System application.

Management's Comments

Management agreed with all the findings and recommendations in the report and disagreed with our estimated other impact of $151.2 million.

In response to recommendation 1, management will configure and update all databases that support the MDIMS application. Management's target implementation date is March 31, 2015.

In response to recommendation 2, management initiated a project to re-enable the [redacted] software on the impacted MDIMS servers. Management's target implementation date is August 31, 2014.

In response to recommendation 3, management are currently remediating vulnerabilities identified in our report and will perform code reviews on MDIMS servers. Management's target implementation date is August 31, 2014.

Management disagreed with the amount of potential risk that exists in the MDIMS and the value of money orders at risk of being fraudulently cashed due to inadequate security controls. Further, management believe that existing controls significantly reduce the risk associated with this estimated cost, including a reconciliation process performed at the accounting service center that identifies money orders sold with invalid serial numbers.

See Appendix G for management's comments, in their entirety.

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 management's disagreement with our estimate of potential risk that exists in the MDIMS, the OIG's calculation of potential risk considered controls that prevent fraud from occurring. Management refers to the money order reconciliation process as a compensating control; however, this process is a detective control that identifies fraudulently issued and cashed money orders after the fraud has occured. Therefore, we believe our estimated value of about $151 million for money orders at risk is reasonable.

The OIG considers recommendations 2 and 3 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

The MDC is a roughly 950,000 square foot warehouse for more than 26,000 different parts, pieces of equipment, and supplies. The MDC performs print services, material distribution, and inventory management for about 31,000 facilities the Postal Service manages. The MDC consists of the following centers:

- The NPC, which prints more than 95 million pages of documents per year, such as manuals, payroll checks, and earning statements.
- The MDC, which processes more than 3.8 million postal-related orders per year, such as parts and supplies.
- The Inventory Control Center, which manages inventory for the Postal Service.

In support of operations, MDC employees and customers use roughly 15 applications to conduct business.

The Postal Service has information security policies to protect applications and data from unauthorized use and modification, including logical controls for protecting applications and information.

Objective, Scope, and Methodology

Our objective was to determine whether electronic safeguards, such as configuring databases, updating operating systems, using [redacted] software, and securing web applications, were in place and operating effectively to protect data from the check printing and inventory management applications against unauthorized modification, loss, and disclosure. We used AppDetective,[25] GFI Languard™,[26] Nessus®,[27] and Hewlett-Packard WebInspect[28] to accomplish our objective.

We performed our work at the Information Technology Service Center in Eagan, MN, and the MDC in Topeka, KS. Our assessment included a review of two IPPD servers and 12 MDIMS servers. We selected the IPPD application because it manages all printers in the NPC that print documents containing sensitive information, such as birth dates and salaries. In addition, we selected the MDIMS application because of the inherent risk associated with using this application to ship blank money order stock to post offices throughout the country. We assessed these servers for vulnerabilities and compliance with Postal Service information security policies and standards. Additionally, we interviewed Postal Service IT staff, assessed scan results, and provided our assessment to Postal Service administrators. See Appendix F for servers tested.

We conducted this performance audit from November 2013 through July 2014, 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 June 11, 2014, and included their comments where appropriate.

---

25 A network-based discovery and vulnerability scanner that discovers database applications within the infrastructure and assesses their security strength. It scans databases for vulnerabilities, configuration issues, weak passwords, missing patches, access control concerns, and other issues that can lead to user privilege escalation.
26 A network security scanner and patch management tool that allows the ability to scan, detect, assess, and rectify security vulnerabilities.
27 A vulnerability and configuration assessment product that features high-speed discovery, configuration auditing, asset profiling, sensitive data discovery, patch management integration, and vulnerability analysis.
28 An automated and configurable web application security and penetration testing tool that mimics real-world hacking techniques and attacks, enabling the user to thoroughly analyze complex web applications and services for security vulnerabilities.

We assessed the reliability of operating system and database configuration data by performing electronic testing of the hosts, reviewing resultant data for false positives and other anomalies, and interviewing agency officials knowledgeable about the data. We determined that the data were sufficiently reliable for the purposes of this report.

Prior Audit Coverage

Report Title	Report Number	Final Report Date	Monetary Impact
Fiscal Year 2012 Information Technology Internal Controls	IT-AR-13-003	1/28/2013	None
Report Results: The infrastructure-level internal controls we tested were properly designed and generally operating effectively; however, we identified several opportunities to strengthen certain infrastructure-level internal controls. Specifically, management could strengthen security monitoring of operating system and database activity, better segregate duties for administrators, ensure effective use of intrusion detection and prevention software, and improve the process for monitoring UNIX and Windows server compliance with operating system configuration requirements. The control weaknesses identified, alone or collectively, did not prevent reliance on infrastructure-level internal controls for the accuracy and timeliness of financial reporting. Management agreed with the findings and recommendations.			
Fiscal Year 2011 Information Technology Internal Controls	IT-AR-12-003	1/9/2012	None
Report Results: The infrastructure level internal controls we tested were properly designed and were generally operating effectively; however, we identified opportunities for management to strengthen certain internal controls over operating systems, databases, data transfer services, job scheduling, and data backup and restoration operations. In addition to the issues identified in Fiscal Year (FY) 2011, we reported on the status of unresolved issues from the FY 2010 review. Management agreed with the recommendations.			

Appendix B: Patch Management Compliance Issues

Table 3 describes software updates for the vulnerabilities detailed in Table 1 relevant to the IPPD application. During our audit, management took corrective action on all critical and high-risk updates noted in Table 4 for the [redacted] and [redacted] servers.

Table 3: Software Updates - Topeka IPPD

No.	Missing Critical and High-Risk Updates	Risk Factor
1	[redacted]	Critical
2	[redacted]	Critical
3	[redacted]	Critical
4	[redacted]	Critical
5	[redacted]	High
6	[redacted]	Critical
7	[redacted]	High
8	[redacted]	Critical
9	[redacted]	Critical
10	[redacted]	High
11	[redacted]	High
12	[redacted]	High
13	[redacted]	Critical
14	[redacted]	High

Source: OIG Nessus and GFI LanGuard scanning tool results.

Table 4 describes software updates shown in Table 1 relevant to the MDIMS application. During our audit, management took corrective action on all critical and high-risk updates noted in the table below for the following servers:

[redacted]

Table 4: Software Updates - MDIMS

No.	Missing Critical and High-Risk Updates	Risk Factor
1	[redacted]	Critical
2	[redacted]	High
3	[redacted]	High
4	[redacted]	High
5	[redacted]	Critical
6	[redacted]	High
7	[redacted]	Critical
8	[redacted]	Critical
9	[redacted]	None
10	[redacted]	High
11	[redacted]	Critical
12	[redacted]	Critical
13	[redacted]	Critical
14	[redacted]	Critical
15	[redacted]	Critical
16	[redacted]	Critical
17	[redacted]	Critical
18	[redacted]	Critical
19	[redacted]	Critical
20	[redacted]	Critical
21	[redacted]	Critical
22	[redacted]	Critical

No.	Missing Critical and High-Risk Updates	Risk Factor
23	[redacted]	Critical
24	[redacted]	Critical
25	[redacted]	High
26	[redacted]	High
27	[redacted]	High
28	[redacted]	High
29	[redacted]	Critical
30	[redacted]	Critical
31	[redacted]	Critical
32	[redacted]	Critical
33	[redacted]	Critical
34	[redacted]	Critical
35	[redacted]	Critical
36	[redacted]	Critical
37	[redacted]	Critical
38	[redacted]	Critical
39	[redacted]	Critical
40	[redacted]	Critical
41	[redacted]	Critical
42	[redacted]	Critical

Source: OIG Nessus and GFI LanGuard scan results.

Appendix C: [redacted] Database Compliance Issues

Table 5 summarizes 15 unique compliance checks and configurations that the OIG's automated scans determined were not compliant with the S*ecurity Hardening Standards for* [redacted] *Databases*. For example, server [redacted] profile was not configured to [redacted] as specified in the hardening standards.

Table 5. [redacted] Database Compliance Issues – MDIMS Application

Category	Vulnerability Checks and Noncompliance Issues Description	MDIMS Application		
		[redacted]		[redacted]
Profiles				
	[redacted]	x	x	x
	[redacted]	x	x	x
Startup Parameter Settings				
	[redacted]	x	x	x
	[redacted]	x	x	x
	[redacted]	x	x	x
Restrict Network Access				
	[redacted]	x	x	x
General Application Configuration Requirements				
	[redacted]	x	x	x
	[redacted]	x	x	x
	[redacted]	x	x	x
	[redacted]	x	x	x
	[redacted]	x	x	x
	[redacted]	x	x	x
	[redacted]	x	x	x
Use of Roles				
	[redacted]	x	x	x
	[redacted]	x	x	x
	Total	**15**	**15**	**15**

Source: AppDetective and Nessus scanning tools results.

Appendix D: Hardening Standards

Table 6 summarizes the compliance checks that the OIG performed to determine if servers running the [redacted] operating system were compliant with Postal Service hardening standards. The "●" in the table identifies those servers that were compliant with hardening standards. The "■" in the table identifies those servers that were not compliant with hardening standards. Specifically, our scans identified two servers, [redacted] and [redacted], that did not have an approved [redacted] software enabled. Both servers had the [redacted] version [redacted] installed, but the software was not enabled. In addition, the servers did not have version [redacted] or version [redacted] installed. In its security advisory [redacted], the vendor recommends that an agency such as the Postal Service install version [redacted] or version [redacted].

Table 6. MDIMS Application Servers running [redacted] operating system

COMPLIANCE CHECK	SERVER NAME [redacted]
Password Management	
Enforced Password History	● ● ● ● ● ● ● ● ● ● ● ●
Maximum Password Age	● ● ● ● ● ● ● ● ● ● ● ●
Minimum Password Age	● ● ● ● ● ● ● ● ● ● ● ●
Minimum Password Length	● ● ● ● ● ● ● ● ● ● ● ●
Default Accounts Locked/ Password Changed	● ● ● ● ● ● ● ● ● ● ● ●
Audit Policy	
Audit Account Logon Events	● ● ● ● ● ● ● ● ● ● ● ●
Audit Account Management	● ● ● ● ● ● ● ● ● ● ● ●
Audit Directory Service Access	● ● ● ● ● ● ● ● ● ● ● ●
Audit Logon Events	● ● ● ● ● ● ● ● ● ● ● ●
Audit Object Access	● ● ● ● ● ● ● ● ● ● ● ●
Audit Policy Change	● ● ● ● ● ● ● ● ● ● ● ●
Audit Privilege Use	● ● ● ● ● ● ● ● ● ● ● ●
Audit Process Tracking	● ● ● ● ● ● ● ● ● ● ● ●
Audit System Events	● ● ● ● ● ● ● ● ● ● ● ●
[redacted]	
[redacted]	● ● ● ● ● ● ■ ■ ● ● ● ●
[redacted]	● ● ● ● ● ● ■ ■ ● ● ● ●
[redacted]	● ● ● ● ● ● ● ● ● ● ● ●

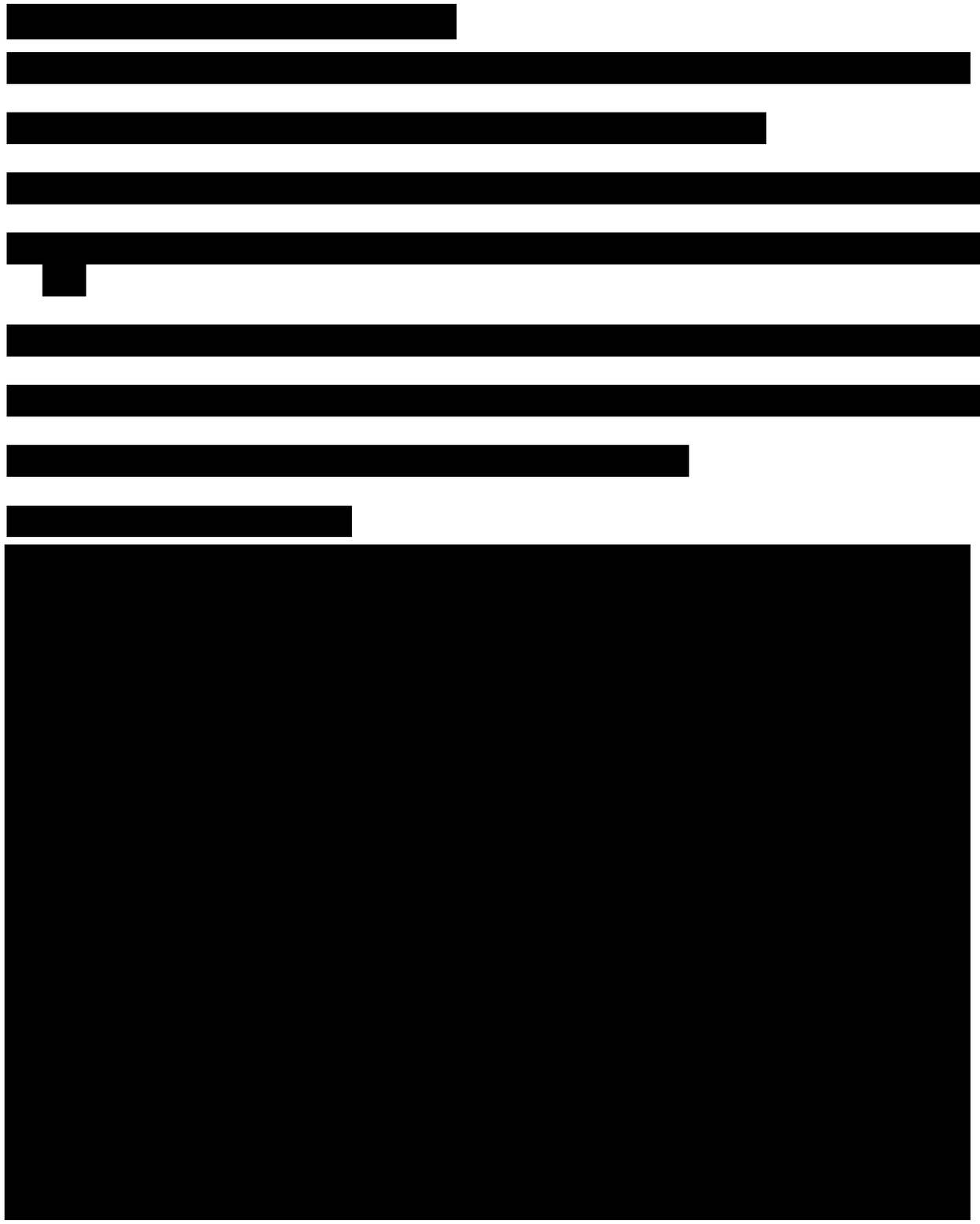
Source: OIG Nessus and GFI LanGuard scanning tools results

Appendix E:
Web Vulnerabilities
Examples

[redacted]

29 A worldwide organization focused on improving the security of software.

[redacted]



[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

31 A global management consulting firm focused on information security.

Appendix F:
Sample Selection Summary

Table 7 identifies the 14 servers we judgmentally selected for testing and the associated application or function residing on each server. We used automated scanning tools to evaluate each server's security.

Table 7. Servers/Applications/Functions

No.	Operating System	IP Address	Server Name	Application/Function
1	[redacted]	[redacted]	[redacted]	IPPD Print Server
2	[redacted]	[redacted]	[redacted]	IPPD Print Server
3	[redacted]	[redacted]	[redacted]	MDIMS Database Server
4	[redacted]	[redacted]	[redacted]	MDIMS Database Server
5	[redacted]	[redacted]	[redacted]	MDIMS Application Server
6	[redacted]	[redacted]	[redacted]	MDIMS Application Server
7	[redacted]	[redacted]	[redacted]	MDIMS Application Server
8	[redacted]	[redacted]	[redacted]	MDIMS Application Server
9	[redacted]	[redacted]	[redacted]	MDIMS Database Server
10	[redacted]	[redacted]	[redacted]	MDIMS Database Server
11	[redacted]	[redacted]	[redacted]	MDIMS Application Server
12	[redacted]	[redacted]	[redacted]	MDIMS Web Server
13	[redacted]	[redacted]	[redacted]	MDIMS Web Server
14	[redacted]	[redacted]	[redacted]	MDIMS Database Server

Source: Servers selected for audit by OIG.

Appendix G: Management's Comments

JOHN T. EDGAR
VICE PRESIDENT
INFORMATION TECHNOLOGY

UNITED STATES POSTAL SERVICE

June 30, 2014

JUDITH LEONHARDT
DIRECTOR, AUDIT OPERATIONS

SUBJECT: Response to Draft Audit Report - Topeka, KS, Material Distribution Center – Information Technology Logical Access Controls (IT-AR-14-DRAFT)

Management agrees with the OIG's findings. The Material Distribution Center (MDC) did not adequately safeguard the 14 servers that support the check printing and inventory management applications, thereby jeopardizing the security of their data.

Specifically, management did not update the operating systems on any of the 14 servers or configure three database servers in accordance with security standards. In addition, the MDC did not use [redacted] software on two servers or adequately protect [redacted] server from unauthorized use.

Management agrees to properly configure databases, verify the latest and approved [redacted] software is enabled on operating systems, and develop a process to ensure security configurations are reviewed on all web servers.

However, management disagrees with the amount of potential risk that exists within the U.S Postal Service's Material Distribution and Inventory Management System (MDIMS) and the value of orders at risk of being fraudulently obtained and cashed if MDIMS data is compromised. The OIG has estimated that $151,238,000 (see Appendix B of the audit report) is potentially at risk due to inadequate security controls. The USPS believes that this amount is grossly over-estimated. It is the USPS's position that the OIG did not properly account for other existing internal controls that would substantially reduce the risk of fraudulent money orders. For example, the Accounting Service Center (ASC) is currently performing a reconciliation process that will identify money orders that are sold with invalid/fraudulent serial numbers. This process would also identify money orders that are being sold via an unidentified POS system/unit etc.

Recommendation 1:

Configure and update all database servers that support the Material Distribution and Inventory Management application.

Management Response/Action Plan:

Management agrees with this recommendation. All required DBMS configuration changes and updates will be made as a part of the MDIMS [redacted] forms upgrade and [redacted] migration initiative.

Target Implementation Date: 3/31/2015

Responsible Official: [redacted], Manager, Eagan Solutions Center

475 L'ENFANT PLAZA SW
WASHINGTON DC 20260-2100
202-268-3977
FAX: 202-268-4492
JOHN.T.EDGAR@USPS.GOV
WWW.USPS.COM

Recommendation 2:

Verify the latest approved [redacted] software is enabled on all servers supporting the Material Distribution and Inventory Management System application.

Management Response/Action Plan:

Management agrees with this recommendation. The vendor software compatibility issue, that caused the [redacted] to be turned off in production, has been resolved. USPS has initiated a project to move this fix into production and re-enable the [redacted] on the impacted MDIMS servers.

Target Implementation Date: 8/31/2014

Responsible Official: [redacted] Manager, Eagan Solutions Center

Recommendation 3:

Review security codes on all web servers that support the Material Distribution and Inventory Management System application.

Management Response/Action Plan:

Management agrees with this recommendation. The identified eMDIMS [redacted] web vulnerabilities are currently being remediated. Once testing is completed the corresponding fixes will be moved into production. In the future eMDIMS code reviews will be performed and coordinated through the Corporate Information Security Office (CISO) using the WebInspect tool. Any web vulnerabilities identified will be remediated as required.

Target Implementation Date: 8/31/2014

Responsible Official: [redacted] Manager, Eagan Solutions Center

This report contains information which management believes may contain proprietary or other business information that may be exempt from disclosure under the Freedom of Information Act (FOIA). Attached is the report detailing the exact information that should be redacted.

John T. Edgar, Vice President, Information Technology

cc:
Sally Haring
William Koetz
Reilly Mitchell
Corporate Audit and 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