OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

Information Storage Security

Audit Report

Report Number
IT-AR-14-004-DR

March 27, 2014

OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

Highlights

The Postal Service spends about $30 million annually on storage components that support 230 systems containing various categories of data which have different protection requirements based on their level of sensitivity. A system outage in 2010 revealed the storage environment was never subject to security reviews or audits, and there were no periodic employee access reviews.

Background

The U.S. Postal Service Information Technology, Computer Operations, Data Management Services group manages a [redacted] petabyte storage environment (equating a byte to 1 second, a petabyte is 35.7 million years). This environment supports 230 systems and applications containing various categories of data, such as personal employee information, which have different protection requirements that reflect their level of sensitivity. The Postal Service spends about $30 million annually on storage components.

The Data Management Services group includes two storage teams – Storage Deployment and Architecture – which manage storage-based hardware in the non-mainframe environment. [redacted]

A system outage in 2010 revealed that Postal Service storage environments were never subject to security reviews or audits. Our objective was to assess the security of information storage environments managed by this group.

What The OIG Found

The Data Management Services group did not manage the storage environment in accordance with Postal Service security requirements because its managers did not provide adequate oversight of the storage teams. They did not, for example, conduct periodic employee access reviews. The absence of proper security practices and training increases the likelihood of an adverse impact on Postal Service operations, such as an outage of a customer-dependent system.

In addition, the Corporate Information Security Office did not provide guidance for storage environments as it has for operating systems, databases, and telecommunication security. Establishing minimum security expectations for storage environments can reduce the likelihood of critical system and application outages throughout Postal Service operations.

What The OIG Recommended

We recommended management establish operating procedures and security requirements and improve oversight of storage environments. We recommended management also ensure personnel are trained to maintain storage skills. In addition, we recommended management develop a schedule to bring the storage environment into compliance with established requirements. Finally, we recommended the Corporate Information Security Office establish security requirements for storage environments.

Transmittal Letter

OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

March 27, 2014

MEMORANDUM FOR: JAMES P. COCHRANE
CHIEF INFORMATION
OFFICER AND EXECUTIVE VICE PRESIDENT

JOHN T. EDGAR
VICE PRESIDENT, INFORMATION TECHNOLOGY

E-Signed by Sean Balduff
VERIFY authenticity with eSign Deskto

for

FROM: John E. Cihota
Deputy Assistant Inspector General
for Financial and Systems Accountability

SUBJECT: Audit Report – Information Storage Security
(Report Number IT-AR-14-004)

This report presents the results of our audit of Information Storage Security (Project Number 13BG010IT000).

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

Cover
Highlights 1
Background 1
What The OIG Found 1
What The OIG Recommended 1
Transmittal Letter 2
Findings 4
Introduction 4
Conclusion 4
Data Management Services' Oversight of Storage Teams 5
Guidance for Storage Environments 6
Recommendations 7
Management's Comments 7
Evaluation of Management's Comments 8
Appendices 9
Appendix A: Additional Information 10
Background 10
Objective, Scope, and Methodology 10
Prior Audit Coverage 11
Appendix B: Data Management Services' Management Oversight 12
Appendix C: Management's Comments 15
Contact Information 18

Findings

The Data Management Services group did not manage the storage environment in accordance with Postal Service security requirements, and its managers did not provide adequate oversight of the storage teams.

Introduction

This report presents the results of our self-initiated audit of Information Storage Security (Project Number 13BG010IT000). Our objective was to assess the security of information storage environments managed by the U.S. Postal Service Information Technology (IT), Computer Operations, Data Management Services (DMS) group. See Appendix A for additional information about this audit.

In January 2013, the Postal Service's DMS group managed over [redacted] petabytes[1] (PB) of enterprise-level storage at the IT Centers (ITC) in [redacted]. Over the past 5 years, Computer Operations has reduced its physical storage footprint by 50 percent and doubled the amount of storage space. By the end of calendar year 2013, the amount of storage space managed had increased to [redacted].

The storage group was composed of about [redacted] on three teams: DMS Architecture, DMS Storage Deployment, and DMS Mainframe Storage. This audit focused on the DMS Architecture and DMS Storage Deployment teams, which manage storage in the non-mainframe environment.[2] The DMS Architecture team is responsible for managing the configuration of most of the storage hardware, managing the storage switches, and designing and maintaining the architectural records for the environment. The DMS Storage Deployment team fulfills requests for storage by application owners and manages the remaining storage hardware. Team members reside at the [redacted]

Roughly [redacted][3] of the two storage teams are contractors – with the majority of personnel provided by the storage hardware vendor, [redacted]. According to the storage contract, [redacted] is responsible for determining the training necessary to fulfill the contract requirements; and for tracking the training, skills, education, and experience of the personnel provided. Postal Service management is responsible for ensuring all personnel under its supervision, including contractors, receive information security training. In addition, management is responsible for maintaining training records and supervising information security responsibilities of its onsite personnel.

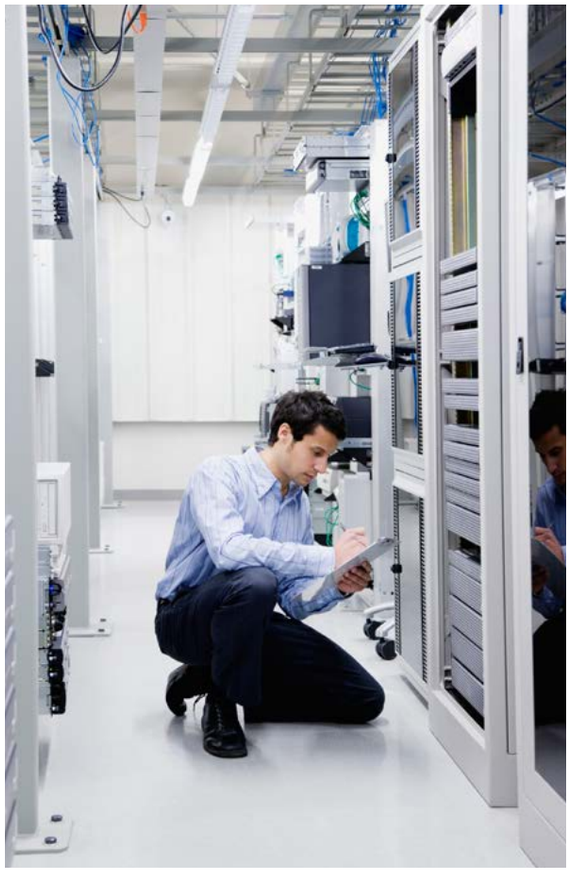
Our audit of a system outage in 2010 revealed that Postal Service storage environments were not subject to external security reviews or audits.[4] Specifically, the Postal Service experienced a 4-day outage of [redacted] in February 2010 due to an incorrect command executed in the storage environment. As a result, the Postal Service incurred additional employee overtime and contractor costs for inputting a backlog of postage statements and restoring [redacted] services. The extra costs incurred by customers to complete the interim manual process negatively impacted the Postal Service brand and goodwill. In addition, the Postal Service recognized revenue late, which could have had an adverse affect on financial reporting had the outage occurred at the end of a quarter or fiscal year.

Conclusion

The DMS group did not manage the storage environment in accordance with established policies. This occurred because DMS managers did not provide adequate oversight of the storage environment teams, such as [redacted] or conducting periodic employee access reviews. In addition, the Corporate Information Security Office (CISO) did not provide adequate guidance for securing storage-based information resources.[6] [redacted] has noted that organizations often overlook security controls in storage environments.The absence of proper security practices increases the likelihood of an adverse impact on Postal Service operations, such as an outage of a customer-dependent system.

---

1 A PB is a measure of memory or storage capacity and is equal to 1 million gigabytes. Equating a byte to 1 second, a PB would equal 35.7 million years.
2 We did not review storage in the mainframe environment in detail since tests of controls in this area were performed in concurrent fiscal year (FY) 2013 audit projects.
3 [redacted] members are contractors, including [redacted] from [redacted] and [redacted].
[redacted]
6 Information resources are all Postal Service information assets, including information systems, hardware, software, data, applications, telecommunications networks, and related resources and the information they contain.



Data Management Services' Oversight of Storage Teams

DMS personnel did not manage the storage environment in accordance with the security requirements outlined in Postal Service Handbook AS-805.[7] DMS managers did not adequately oversee the storage teams and failed to develop security operating procedures and monitor operational security training. The absence of proper security practices and training increases the likelihood of an adverse impact on Postal Service operations, such as an outage of a customer-dependent system like the one used to manage customers' changes of address.

The absence of adequate DMS management oversight was evident in the following ways:

- Implementation of Handbook AS-805 — We noted 20 examples in [redacted] security areas [redacted] where DMS personnel were not informed how to administer storage resources in accordance with Handbook AS-805. For example, administrators were not informed how to ensure that a user formally requests account access and receives a manager's review or approval before an administrator creates an account on a storage device. In addition, there was no evidence that DMS managers periodically reviewed access granted to their team members as required by Handbook AS-805. We identified 31 user accounts that either remained on four types of devices as duplicates or were not removed after the owners no longer had storage responsibilities. We also identified eight default accounts with default passwords remaining on four types of storage devices. The majority of the storage team members were contractors, and managers are required to supervise the information security responsibilities of onsite contractors under their supervision.

- Monitoring of Training — We noted two examples in separate security areas where storage administrators were not familiar with a new management tool or a change in vendor guidance. In one example, DMS implemented the [redacted] in its storage environments.[9] [redacted] strongly recommends that customers enable the [redacted] feature to provide access authorization and activity-logging capabilities (required under Postal Service policy) when the [redacted] is installed. The DMS storage administrators elected not to enable the feature due to concerns that the storage environment lacks 24-hour support. They were not aware the feature could be configured to provide the same level of remote access previously provided to [redacted] without requiring 24-hour support by the Postal Service. Postal Service IT policies dictate that business and line managers and supervisors are responsible for ensuring all personnel under their supervision receive information security training. In addition, these managers are responsible for maintaining training records and supervising information security responsibilities of their onsite contractor personnel.

See Appendix B, Table 1 for a complete list of the security areas and examples of noncompliance noted during the audit.

Storage environments are subject to numerous risks, including data loss or exposure, system outages, and data corruption. In the event of a storage-related outage, the Postal Service would likely experience additional overtime and contractor costs related to restoring the system, plus potential manual processing efforts. In addition, if an outage were to occur at the end of a quarter or fiscal year, financial reporting could be adversely impacted by late recognition of revenue. This project did not disclose any specific risk with particular applications or systems. The potential costs or lost revenue would vary widely depending on the system impacted, the length of an outage, and recoverability of lost or corrupted data. Further, any of these conditions during a peak volume period would likely attract negative press, impact customer satisfaction, and harm the Postal Service's goodwill and brand.

7 Postal Service Handbook AS-805, Information Security, May 2013, Sections 2-2.10, 8-5.4.3, and 8-5.4.4.
[redacted]

9 The [redacted] provides [redacted] with secure access to remotely monitor and respond to potential problems with its customers' storage devices.

Guidance for Storage Environments

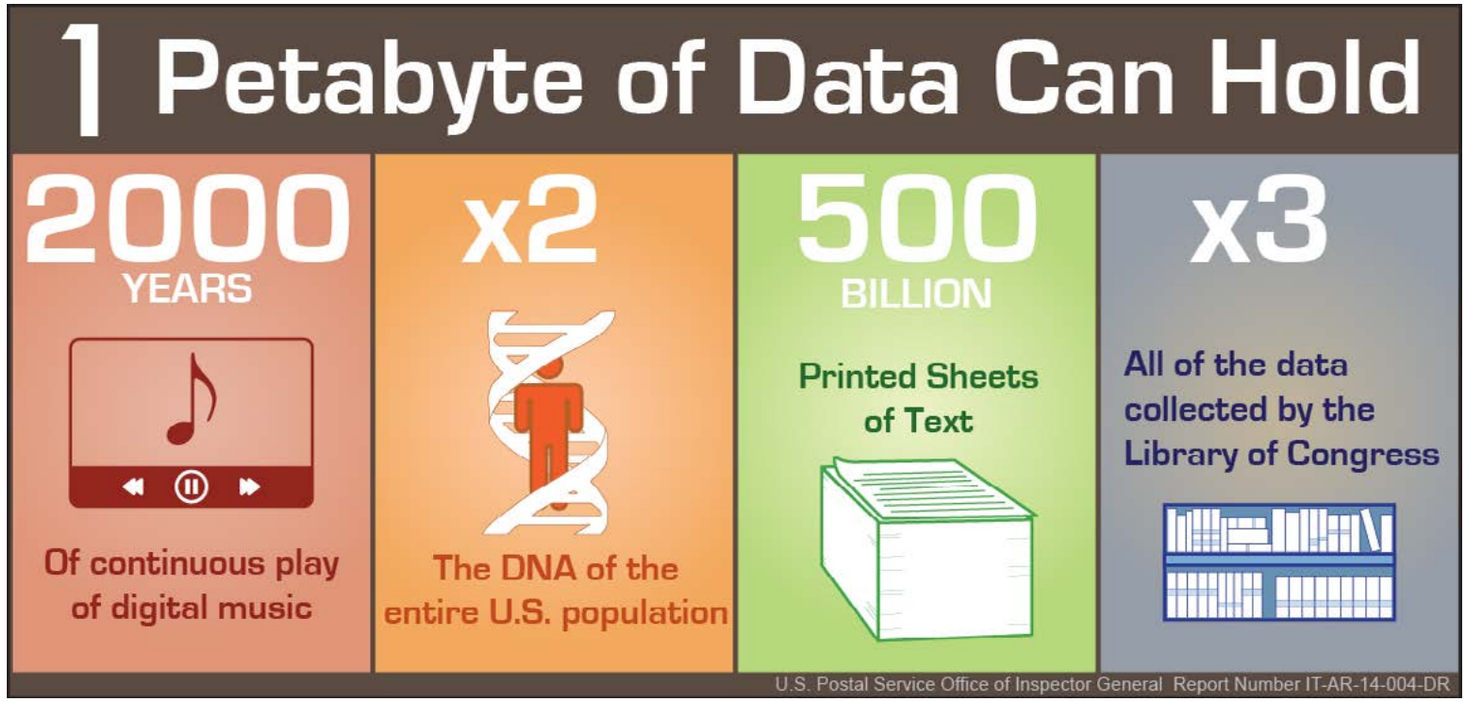
CISO did not provide adequate guidance for securing storage-based information resources. Current Postal Service policy requires that hardware and system software be configured to information security requirements specific to the Postal Service.[10] Policy also establishes that CISO is responsible for developing detailed guidance in the form of handbooks, standards, practices, and hardening[11] policies. [redacted] notes that, while companies often overlook storage security controls, leading enterprises are expanding security strategies to include more direct protection.

We identified areas where additional guidance for storage environments would improve security operations. For example:

- DMS-managed storage devices are not synchronized to a trusted, internal Postal Service time source. Some devices are synchronized to the vendor's time source. A common, accurate time source across the Postal Service environment would ensure that event records from different sources or devices can be correlated when necessary.

- Storage devices designated by DMS as supporting non-production environments were found to be supporting environments considered production environments by their owners. We found the definition of a "production" or a "non-production" environment changed based on the function of the speaker – that is, the storage team, operating system administrator, or application owner. For example, the business team for one application considered the servers used for training to be part of a production environment, and expected related devices to be treated as production from a support and maintenance perspective. However, the DMS storage team was managing the associated storage device as a "non-production" device. The primary impact of a "production" versus "non-production" designation is whether the stored data is copied and incorporated into disaster recovery procedures.

[redacted] promotes security best practices that move beyond a perimeter defense and build security into the storage infrastructure. By establishing the minimum security expectations for storage environments, CISO can reduce the likelihood of critical system outages or corrupted data throughout Postal Service operations. See Appendix B, Table 2 for examples of areas where additional guidance of storage environments would improve security operations.



10 Handbook AS-805, Sections 2-2.5 and 8-2.4.2, establish CISO's responsibility for developing information security guidance and the requirement for hardware and software hardening.
11 Hardening is the process of implementing software, hardware, or physical security controls to mitigate risks associated with the Postal Service infrastructure and critical and sensitive information resources.

Recommendations

The OIG made 5 recommendations to improve the security of information storage and help ensure adequate procedures, training, and oversight.

We recommend the vice president, Information Technology, direct the manager, Computer Operations, to:

1. Ensure Data Management Services management provides security operating procedures, periodic reviews, and oversight for the storage teams as required by Handbook AS-805, Information Security.

2. Ensure the vendor for the storage contract provides periodic training to personnel to maintain storage group knowledge and skills with vendor products and management tools.

3. Evaluate the storage environment managed by Data Management Services against Handbook AS-805, Information Security, security requirements and develop a schedule to bring the environment into compliance.

We recommend the chief information officer and executive vice president direct the manager, Corporate Information Security, to:

4. Establish minimum security requirements for storage devices in Postal Service environments based on industry best practices.

5. Specifically address storage devices and storage environment security requirements within Handbook AS-805, Information Security, to reflect the significance of these infrastructure components. This should include guidance on consistent use of production and non-production designations among storage teams and application owners.

Management's Comments

Management agreed with all the findings and recommendations in the report. In response to recommendation 1, management is planning to register resources and roles in the eAccess system to facilitate regular access reviews. The planned implementation date is September 30, 2014.

In response to recommendation 2, management will work with the contracting officer to receive quarterly training reports beginning April 1, 2014.

In response to recommendation 3, management will develop a gap analysis by May 1, 2014, and provide a plan for corrective actions to the U.S. Postal Service Office of Inspector General (OIG) by June 1, 2014.

In response to recommendation 4, management from Computer Operations and CISO will coordinate to establish minimum security requirements for storage in Postal Service environments by September 30, 2014.

In response to recommendation 5, management will update Handbook AS-805, *Information Security*, to address storage devices and storage environment security requirements by September 30, 2014.

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

Evaluation of Management's Comments

The OIG considers management's comments responsive to recommendations 2 through 5 and the corrective actions should resolve the issues identified in the report. Regarding recommendation 1, management's comments address the recommended periodic reviews, but do not specifically discuss actions to implement security operating procedures or oversight for the storage teams. Since security operating procedures and oversight are required by Handbook AS-805, the OIG will monitor implementation and compliance for these items through the gap analysis and plan for corrective actions outlined in management's response to recommendation 3.

The OIG considers recommendations 1 through 4 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 10
Background 10
Objective, Scope, and Methodology 10
Prior Audit Coverage 11
Appendix B: Data Management Services' Management Oversight 12
Appendix C: Management's Comments 15

Appendix A: Additional Information

Background

At the end of December 2013, DMS managed about [redacted] PB of enterprise-level storage[12] at the ITCs in [redacted]. The Postal Service spends about $30 million annually on storage components.

The DMS-managed storage devices support 230 production IT systems and applications running on over 1,100 servers[13] at the [redacted] ITCs. For example, these devices store data for the systems used to process biweekly payroll for Postal Service employees and to manage changes of address for Postal Service customers. The devices also support non-production systems and environments. Each of the storage devices has a combination of numerous categories of stored data[14] including sensitive data, personally identifiable information, and debit and credit card records. Different categories of data have different protection requirements, including where the data can be accessed, use of encryption, storage location, and retention periods.

Objective, Scope, and Methodology

Our objective was to assess the security of information storage environments managed by DMS. To accomplish our objective, we interviewed officials at Postal Service facilities in [redacted]. We also reviewed applicable Postal Service policies and procedures, guidelines, and reports.

Our review focused on the production storage environment managed by DMS at the [redacted] ITC during FY 2013. The scope of our audit included hardware devices such as disk arrays,[15] servers used for managing the storage environment, and switches controlling the storage network.

In the absence of Postal Service guidance for hardening storage environments, we selected several security hardening topics and reviewed DMS-managed storage devices for compliance. The topics appear in Figure 1.

Figure 1. Hardening Topics Selected for Review

• Change Management Practices	• Modems	• Services and Ports
• Disposal	• Password Polices	• Session Timeout
• Encryption Services	• Patching Practices	• Storage Scripts
• Logging and Log Monitoring	• Role-Based Access Control	• Training and Management Support
• Management Interfaces	• Secure Application Programming Interface	• User Account Management

Source: OIG analysis.

12 Enterprise storage is a broad category that includes products and services used to assist large organizations with large volumes of data and large numbers of users. It usually involves centralized storage repositories.
13 These include host servers, which, in turn, may support multiple virtual servers.
14 The Postal Service is mandated to protect information of its customers, employees, and suppliers, and in order to do so, it categorizes systems and data by sensitive, sensitive-enhanced, personally identifiable information, non-sensitive, debit and credit card records, Privacy Act records, and financial reporting data required to comply with the Sarbanes-Oxley Act of 2002.
15 A disk array is a hardware element that contains a large group of hard disk drives.

We conducted interviews, assessed security configurations from randomly sampled production storage devices and software, reviewed controls over access to stored data, analyzed the storage architecture, and performed other necessary measures to address the audit objectives. The team also contacted Postal Service contracting officers regarding several components of the [redacted] storage contract. We researched and identified nine best practices or norms from sources like the Storage Networking Industry Association (SNIA™) and the National Security Agency, Systems and Network Analysis Center. We coordinated with the Council of the Inspectors General on Integrity and Efficiency and did not identify any audit work performed on the security of storage environments of other agencies.

We conducted this performance audit from July 2013 through March 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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. We discussed our observations and conclusions with management on March 5, 2014, and included its comments where appropriate.

We did not assess the reliability of any computer-processed data for the purposes of this report. The computer-processed data analyzed during the audit provided the context for the environment audited and did not significantly affect the findings, conclusions, or recommendations in this report.

Prior Audit Coverage

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

Appendix B: Data Management Services' Management Oversight

The audit focused on production hardware in the DMS-managed storage environment at the [redacted] ITC. Table 1 lists descriptions of types of noncompliance with Handbook AS-805 across multiple security areas caused by inadequate management oversight. A check (√) under the device type indicates an issue exists with at least one sample of that type.

During the audit, members of the DMS storage teams and others initiated corrective action to address some of the issues we found. These include removing unnecessary and outdated accounts from storage devices, updating the session timeouts on two types of devices, implementing the [redacted] to replace modem access, and conducting a physical inventory of storage devices in the [redacted] ITC.

Table 1: Impact of Inadequate DMS Management Oversight

Section A: Implementation of Handbook AS-805

Description		Device type[1]				
		[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
1 Account management						
1.1	[redacted]	√	√	√	√	√
1.2	[redacted].		√			√
1.3	[redacted]	√		√	√	√
1.4	User accounts are not periodically reviewed.	√	√	√	√	√
1.5	Use of privileged accounts is not restricted.	√	√	√	√	
1.6	Shared account is not registered.	√	√	√		√
2 Password policies						
2.1	[redacted]	√	√	√		√
2.2	Administrator-level accounts had no password expiration.	√		√		
2.3	No documented approval for non-expiring passwords.	√		√		
2.4	[redacted]	√	√			
2.5	No confirmation that vendor defaults comply with Handbook AS-805.	√				
3 Role-based access control						
3.1	No separation of security and administrative duties.[2]	√	√	√	√	√
4 Idle session timeout						
4.1	No idle timeout set.				√	
4.2	No confirmation that vendor defaults comply with Handbook AS-805.	√		√		
5 Patching practices						
5.1	The current process for evaluating [redacted] device and [redacted] (which incorporates reliance on the vendor for certain aspects, such as testing and implementation) is not documented. The current process for evaluating [redacted] patches is not documented.					

1 [redacted] is the contract vendor providing most of the hardware storage devices used by DMS. These include [redacted]

2 Most storage devices give administrators the ability to create custom roles as necessary (the exception is [redacted]. The audit disclosed that vendor default roles were used to grant administrator level authority to accounts regardless of work responsibilities (that is, account owners or users who are assigned to different DMS teams).

Table 1: Impact of Inadequate DMS Management Oversight

6 Use of modems and [redacted]	
6.1	CISO has no record of a DMS request for authorization to use modems. Sixteen of 29 identified modems remain in operation following implementation of the [redacted]. Thirteen of the 16 modems are connected to devices already converted to the [redacted]
6.2	CISO and the Network Connectivity Review Board[3] have no record of a DMS request for the [redacted] used in the non-Payment Card Industry environment.
7 Storage scripts	
7.1	An external review of a sample storage script did not identify any specific concerns. However, based on the extensive use of scripts by the storage teams, security could be enhanced with additional oversight for the use of:
Comments sections that include the purpose, date of creation, author, and platform notes (and change record reference).	
Techniques to avoid hard coding management workstations within scripts.	
8 Asset management	
8.1	DMS records of the devices in the storage environment were generally incomplete. The teams relied on the vendor's account manager for records of the location and status of storage devices. For example, one [redacted] device confirmed during the physical inventory did not appear in the records provided by DMS. In another example, two servers installed as management servers were not identified by DMS until the end of the audit.
8.2	Personnel were unfamiliar with the location, Internet address, or status of a vendor-supplied server connected to the storage environment.

Section B: Monitoring of Training

1 [redacted]	
1.1	[redacted] was not enabled. If enabled, [redacted] could provide compliance with the Postal Service requirement to maintain activity logs and provide authorization control while allowing [redacted] the necessary level of remote access. This would not require 24-hour storage support by the Postal Service.
2 Reliance on outdated commands	
2.1	[redacted] replaced older commands on [redacted] devices with a new tool to manage user accounts. Although the new tool is available to the DMS team, it continues to manage accounts using the older commands.

3 Postal Service Handbook AS-805-D, Information Security Network Connectivity Process, Section 2-6, September 2009, establishes the Board's responsibility for evaluating and approving or rejecting requests for Postal Service connections to external systems, and for reviewing new information resource, infrastructure, and network connections and their effects on overall Postal Service operations and information security.

Source: OIG audit analysis results.

Table 2 provides examples of security areas where additional guidance is needed for protecting storage environments. The CISO needs to establish minimum security requirements for individual storage device types to protect operations and data in the Postal Service environment.

Table 2: Additional Postal Service Guidance is Needed

Security Area	
1 Storage environments discussed in Handbook AS-805	
1.1	Handbook AS-805 does not discuss security for storage environments in a manner that reflects the current role it serves in maintaining computer operations. For example, the Hardware Security section of the handbook discusses mainframes, network devices, servers, workstations, and mobile computing devices; however, there is no section dedicated to storage devices.
2 Specific device guidance – for example, hardening standard or baseline	
2.1	Handbook AS-805 requires hardware and system software to be hardened to Postal Service requirements. Hardening guidance exists for operating systems, databases, network and telecommunications; however, the minimum Postal Service requirements have not been established for storage devices or switches used within storage environments.
3 Interpreting vendor guidance	
3.1	[redacted] guidance for error message logging differs from the Postal Service hardening standard for non-storage switches. All error messages are rated from greatest severity zero (emergencies such that the system is unusable) to least severity seven (debugging messages). The vendor uses severity five (notifications of normal, but significant conditions) as the minimum level to be logged, while the Postal Service standard is for logging messages no lower than severity six (informational messages).
3.2	[redacted] security guidance offers three options for authentication credentials and encourages organizations to determine the best option for their environment. The Postal Service has not determined the best option for the DMS storage environment.
3.3	[redacted] security guidance on accepting connections from remote clients provides parameters to be configured to the organization's acceptable tolerance levels. The Postal Service has not determined the appropriate tolerance levels for the DMS storage environment.
4 Logging practices	
4.1	The SNIA maintains storage security best practices that include a list of the kinds of events that should be logged. The Postal Service has not established the kinds of events to be logged by devices in the DMS storage environment. Therefore, the types of activity and severity levels logged by DMS-managed switches are inconsistent.
4.2	Several types of DMS-managed storage devices retain logs only on the device. SNIA recommends use of centralized audit logging from all sources for automated analysis, alerting, and archiving to support compliance, accountability, and security.
5 Synchronized clocks	
5.1	DMS-managed storage devices are synchronized to either the vendor's time source or to multiple Postal Service time sources. SNIA best practices include use of a common, accurate time source across the environment. While existing hardening standards for other Postal Service resources discuss the use of network time protocol, there is no guidance provided for storage environments.
6 Account management	
6.1	[redacted] devices do not provide the ability to monitor password aging for local accounts. Guidance should be provided on whether these accounts should be submitted for approval as non-expiring password accounts.
7 Script automation	
7.1	Based on the extensive use of scripts and automation, security could be enhanced with additional guidance on the use of:
8 Production versus non-production	
8.1	Storage devices internally designated as non-production were found to be supporting environments considered production by their owners. The definition of what is "production" and "non-production" changes based on the speaker – that is, storage team, operating system administrator, or application owner.
Source: OIG audit analysis results.	

Appendix C: Management's Comments

UNITED STATES POSTAL SERVICE

March 20, 2014

JUDITH LEONHARDT
DIRECTOR, AUDIT OPERATIONS

SUBJECT: Draft Audit Report – Information Storage Security (Report Number IT-AR-14-DRAFT)

Thank you for the opportunity to review and comment on the Information Storage Security draft audit report.

Recommendation 1:
Ensure Data Management Services management provides security operating procedures, periodic reviews, and oversight for the storage teams as required by Handbook AS-805, *Information Security*.

Management Response/Action Plan:
Management agrees with this recommendation and was already in the process of implementing the recommendation at the start of the audit. The current plan centers on completing the work (registering resources and roles) in the PCI environment. Once that is complete, we will replicate that to the rest of the USPS storage environment in eAccess (which will facilitate regular access reviews).

Target Implementation Date:
September 30, 2014

Responsible Official:
Jerry Reynolds, Computer Operations

Recommendation 2:
Ensure the vendor for the storage contract provides periodic training to personnel to maintain storage group knowledge and skills with vendor products and management tools.

Management Response/Action Plan:
Management agrees with the recommendation. We will ask the contracting officer to direct [redacted] to provide quarterly training reports beginning 4/1/14.

Target Implementation Date:
April 1, 2014

Responsible Official:
Jerry Reynolds, Computer Operations

Recommendation 3:
Evaluate the storage environment managed by Data Management Services against Handbook AS-805, Information Security, security requirements and develop a schedule to bring the environment into compliance.

Management Response/Action Plan:
Management agrees with the recommendation. We will develop a gap analysis by 5/1/14 and develop a corrective action plan which will be provided to the OIG by 6/1/14.

Target Implementation Date:
June 1, 2014

Responsible Official:
Jerry Reynolds, Computer Operations

Recommendation 4:
Establish minimum security requirements for storage devices in Postal Service environments based on industry best practices.

Management Response/Action Plan:
Management agrees with this recommendation. Computer Operations and CISO will combine remediation efforts to establish minimum security requirements for storage in Postal Service environments.

Target Implementation Date:
September 30, 2014

Responsible Official:
Chuck McGann, Corporate Information Security Office
Jerry Reynolds, Computer Operations

Recommendation 5:
Specifically address storage devices and storage environment security requirements within Handbook AS-805, Information Security, to reflect the significance of these infrastructure components. This should include guidance on consistent use of production and non-production designations among storage teams and application owners.

Management Response/Action Plan:
Management agrees with this recommendation. CISO will update the Handbook AS-805 to address storage devices and storage environment security requirements. Additionally, CISO will include a clarification between production and non-production designations among storage teams and application owners.

Target Implementation Date:
September 30, 2014

Responsible Official:
Chuck McGann, Corporate Information Security Office

There are no monetary findings in this report.

The subject report and this response contain information related to potential security vulnerabilities that, if released, could be exploited and cause substantial harm to the U.S. Postal Service. The CIO and VP Information Technology request that Appendix B: Data Management Services' Management Oversight of the report be considered as classified, restricted, and exempt from disclosure under the Freedom of Information Act (FOIA).

James P. Cochrane
Chief Information Officer and Executive Vice President

John T. Edgar
Vice President, Information Technology

cc: Sally K. Haring, Manager, 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