



OFFICE OF INSPECTOR GENERAL UNITED STATES POSTAL SERVICE

Privileged Account Management

Audit Report

Report Number
IT-AR-17-003

April 5, 2017





OFFICE OF INSPECTOR GENERAL UNITED STATES POSTAL SERVICE

Highlights

The Postal Service is not effectively managing all privileged accounts in accordance with its policies and best practices.

Background:

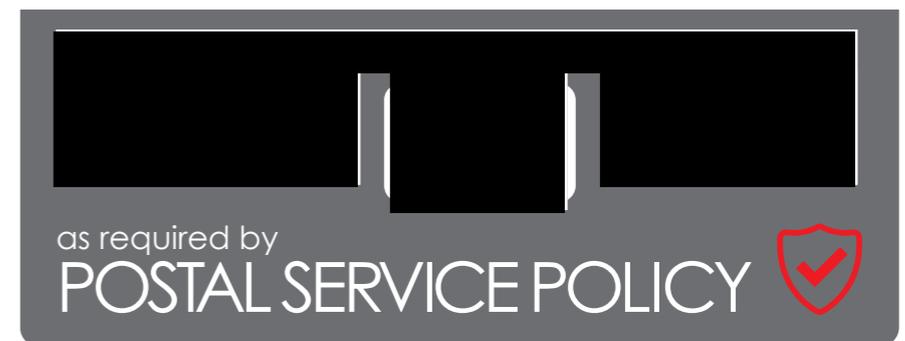
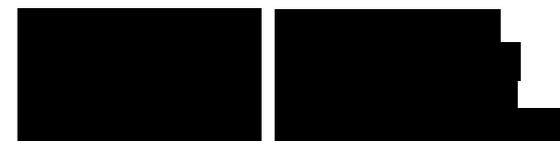
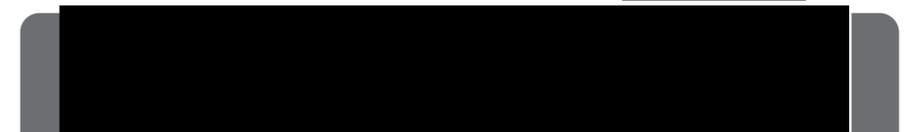
The U.S. Postal Service manages access to information resources using multiple types of accounts, including privileged accounts. Privileged accounts are those that have higher levels of rights such as account creation, update, deletion, or full application functionality. The Postal Service uses both automated and manual processes to manage account access and authorization to information resources. Proper management and monitoring of privileged accounts is important to ensure information is secure and systems and data are not modified without authorization.

Our objective was to determine if the Postal Service is effectively managing privileged accounts in accordance with Postal Service policies and best practices.

What the OIG Found:

The Postal Service is not effectively managing all privileged accounts in accordance with its policies and best practices. Specifically, the Postal Service has not developed adequate guidance and controls to identify and manage privileged accounts. The [redacted] allows for the identification of privileged accounts; however, we found that the Postal Service only used this feature for [redacted] systems. As a result, management could not identify all privileged accounts throughout the Postal Service.

Within 3 systems that did not use the privileged identifier field in [redacted]



We reviewed accounts for three systems that did not use the privileged identifier field in eAccess to determine if controls over privileged accounts existed within each system. We found that [redacted] percent of the users for these three systems did not have proper authorization for privileged accounts and [redacted] percent of



OFFICE OF INSPECTOR GENERAL

UNITED STATES POSTAL SERVICE

the users did not have the appropriate security clearance. Also, users did not always [REDACTED], as required by Postal Service policy.

Management also does not adequately monitor privileged account activity. The owners and administrators of the three systems we reviewed, as well as the Corporate Information Security Office, are not maintaining system and audit logs or tracking privileged users' last logons to monitor user activity, as required by Postal Service policy. We also found the Postal Service does not have a comprehensive training program for all privileged users to ensure they understand their roles, responsibilities, and the risks associated with their elevated privileges.

These issues occurred because:

- Management focused on other areas of cyber security and has not yet developed comprehensive guidance for defining, identifying, and managing privileged accounts.
- System owners did not require all privileged users to follow Postal Service policy when requesting privileged access and did not ensure that users have the appropriate security clearance prior to granting access.
- System owners were not aware of the [REDACTED] [REDACTED] requirement.

- Management has not defined business practices for monitoring privileged accounts or implemented privileged access management tools in accordance with best practices.
- Postal Service policy does not require all privileged users to complete training.

Without proper management of privileged accounts, the Postal Service cannot ensure the confidentiality and integrity of its data, which could lead to data loss and reduced confidence in the Postal Service brand. Without proper monitoring of privileged accounts, the Postal Service cannot ensure privileged users have accountability in order to prevent accidental harm or malicious activity. In addition, the lack of a comprehensive training program for all privileged users exposes the Postal Service to credential or password compromise.

What the OIG Recommended:

We recommended management:

- Strengthen controls over privileged users by continuing to develop overarching guidance and controls for managing privileged accounts that includes establishing a consistent method for identifying all privileged accounts.
- Develop and continuously maintain a complete and accurate listing of privileged accounts for Postal Service systems.



OFFICE OF INSPECTOR GENERAL

UNITED STATES POSTAL SERVICE

- Require all users to follow Postal Service policy when requesting and granting privileged access, ensure privileged users have proper security clearances, and require privileged users to [REDACTED].
- Clearly define the responsibilities for monitoring privileged accounts, implement privileged access management tools, and track privileged users' activity.
- Develop a comprehensive privileged user training program, and require all privileged users to complete the training before assuming their privileged role, followed by periodic refresher training.

Transmittal Letter



OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

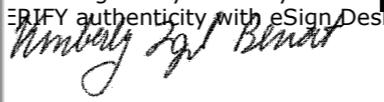
April 5, 2017

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

JEFFREY C. JOHNSON
VICE PRESIDENT, INFORMATION TECHNOLOGY

MICHAEL AMATO
VICE PRESIDENT, ENGINEERING SYSTEMS

WILLIAM C. RUCKER III
SENIOR VICE PRESIDENT, SALES AND
CUSTOMER RELATIONS

E-Signed by Kimberly Benoit
VERIFY authenticity with eSign Desktop


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

SUBJECT: Audit Report – Privileged Account Management
(Report Number IT-AR-17-003)

This report presents the results of our self-initiated audit of the U.S. Postal Service's Privileged Account Management (Project Number 16TG021IT000).

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

Attachment

cc: Corporate Audit Response Management

Table of Contents

Cover	
Highlights.....	1
Background:.....	1
What the OIG Found:.....	1
What the OIG Recommended:.....	2
Transmittal Letter.....	4
Findings.....	6
Introduction.....	6
Summary.....	6
Management of Privileged Accounts.....	7
Monitoring of Privileged Accounts.....	9
Comprehensive Training Program.....	9
Recommendations.....	11
Management’s Comments.....	12
Evaluation of Management’s Comments.....	13
Appendices.....	14
Appendix A: Additional Information.....	15
Background.....	15
Objective, Scope, and Methodology.....	15
Prior Audit Coverage.....	16
Appendix B: Management’s Comments.....	17
Contact Information.....	25

Findings

Introduction

This report presents the results of our self-initiated audit of the U.S. Postal Service's privileged account management (Project Number 16TG021IT000). Our objective was to determine if the Postal Service is effectively managing privileged accounts in accordance with its policies and best practices. See [Appendix A](#) for additional information about this audit.

The Postal Service manages access to information resources using various types of accounts, including privileged accounts. Privileged accounts are those that have higher levels of rights such as account creation, update, deletion, or full application functionality.

Proper management of privileged accounts is important to ensure information is secure and systems and data are not modified without authorization. It is essential for organizations to identify all privileged accounts and their owners, establish privileged access governance, and monitor privileged accounts to reduce the risk of unauthorized access and security incidents.

Summary

The Postal Service is not effectively managing all privileged accounts in accordance with its policies and best practices. Specifically, the Postal Service has not developed adequate guidance and controls to identify and manage privileged accounts. The Postal Service uses both automated and manual processes to manage account access and authorization to information resources. The [REDACTED] [REDACTED] allows for the identification of privileged accounts; however, we found that the Postal Service only used this feature for [REDACTED] systems. In addition, the Postal Service uses the automated [REDACTED] and the manual Postal Service (PS) [REDACTED] as alternative methods for requesting and approving accounts; however, these methods do not have a unique field to identify privileged accounts. As a result, management could not identify all privileged accounts at the Postal Service.

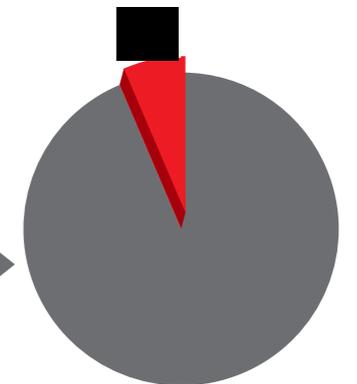
We reviewed accounts for three critical, non-Payment Card Industry Data Security Standard (PCI-DSS), and non-Sarbanes-Oxley Act (SOX) systems⁴ — [REDACTED]

The automated access request system allows for the identification of privileged accounts

We found that

The Postal Service only used this feature for

SYSTEMS



1 The Postal Service's application for managing account access and authorization to information resources.
2 [REDACTED] is used to request access to information resources on the U.S. Postal Inspection Service domain.
3 Used to request access to information resources not available within [REDACTED].
4 PCI-DSS is a widely accepted set of policies and procedures intended to optimize the security of credit, debit, and cash card transactions and protect cardholders against misuse of their personal information. SOX is a federal law protecting investors from the possibility of fraudulent accounting activities by corporations and requiring management to certify the accuracy of their reported financial statements.
5 [REDACTED] provides [REDACTED] customer service by [REDACTED] across the organization.
6 A system used for both inbound and outbound [REDACTED].

The Postal Service is not effectively managing all privileged accounts in accordance with its policies and best practices. Specifically, the Postal Service has not developed adequate guidance and controls to identify and manage privileged accounts.

██⁷ — that did not use the privileged identifier field in ██████████ to determine if controls over privileged accounts existed in each system. We found that users did not always have proper authorization for privileged accounts, have the appropriate security clearance, or ██████████

In addition, management does not adequately monitor privileged accounts. Specifically, the owners and administrators of the three systems we reviewed, as well as the Corporate Information Security Office (CISO), are not maintaining system and audit logs or tracking privileged users' last logons to monitor user activity. In addition, the Postal Service does not have a comprehensive training program for all privileged users to ensure they understand their roles, responsibilities, and the risks associated with their elevated privileges.

These issues occurred because management focused on other areas of cyber security and has not yet developed comprehensive guidance for defining, identifying, and managing privileged accounts. System owners did not require all privileged users to follow Postal Service policy when requesting privileged access and did not ensure that users have the appropriate security clearance prior to granting access. System owners were also not aware of the ██████████ requirement.

In addition, management has not defined business practices for monitoring privileged accounts or implemented privileged access management tools in accordance with best practices. Further, privileged user training was not implemented because Postal Service policy does not require all privileged users to complete it.

Without proper management of privileged accounts, the Postal Service cannot ensure the confidentiality and integrity of its data, which could lead to data loss and reduced confidence in the Postal Service brand. Without proper monitoring of privileged accounts, the Postal Service cannot ensure privileged users have accountability in order to prevent accidental harm or malicious activity. In addition, the lack of a comprehensive training program for all privileged users exposes the Postal Service to credential or password compromise.

Management of Privileged Accounts

The Postal Service is not effectively managing all privileged accounts in accordance with its policies and best practices. Specifically, the Postal Service has not developed adequate guidance and controls to identify and manage privileged accounts. For instance, the Postal Service has not clearly defined the term "privileged account" or established a method to identify and manage all privileged accounts.

The ██████████ application allows for the identification of privileged accounts; however, we found the Postal Service was only using this feature for ██████████). In addition, the Postal Service uses the automated ██████████ application and the manual PS Form ██████████ as alternative methods for requesting and approving accounts; however, these methods do not have a unique field to identify privileged accounts. As a result, management could not identify all Postal Service privileged accounts.

⁷ A system that incorporates advanced technology to consolidate and provide ██████████

We also reviewed privileged accounts for three critical systems — [REDACTED] — that did not use the privileged identifier field in [REDACTED] to determine if controls over these privileged accounts existed in each system.⁸ We found that system owners inconsistently managed privileged accounts. Specifically, privileged users did not always have proper authorization for privileged accounts and did not always have the appropriate security clearance. Table 1 and Table 2 summarize our results.

Table 1. Privileged Accounts with Unauthorized⁹ Access

Systems	Number of Accounts Without Proper Authorization	Total Number of Privileged Accounts Reviewed	Percentage of Accounts Without Proper Authorization
[REDACTED]	[REDACTED]	159	[REDACTED]
[REDACTED]	[REDACTED]	25	[REDACTED]
[REDACTED]	[REDACTED]	2	[REDACTED]
Total	[REDACTED]	186	[REDACTED]

Source: U.S. Postal Service Office of Inspector General (OIG) analysis.

Table 2. Privileged Users without a Security Clearance

Systems	Number of Privileged Users Without a Security Clearance	Total Number of Privileged Users Reviewed	Percentage of Privileged Users Without a Security Clearance
[REDACTED]	[REDACTED]	96	[REDACTED]
[REDACTED]	[REDACTED]	25	[REDACTED]
[REDACTED]	[REDACTED]	2	[REDACTED]
Total	[REDACTED]	123	[REDACTED]

Source: OIG analysis.

Furthermore, privileged users for [REDACTED] and [REDACTED] did not [REDACTED] as required by policy. According to best practices,¹⁰ organizations should establish a privileged access governance model that includes establishing guidance and controls for managing accounts and identifying all privileged accounts and their owners within the organization. Postal Service policy¹¹ requires users to request authorization for access to information resources through [REDACTED]. If the information resource is not available within [REDACTED], the user must request it using a PS Form [REDACTED]. In addition, Postal Service policy¹² requires personnel with access to sensitive or critical resources to obtain appropriate clearances and privileged users to [REDACTED].

⁸ Since the Postal Service did not define privileged accounts or use the privileged identifier field in [REDACTED] to indicate privileged users, the OIG requested a list of privileged accounts. In response to our request, the Postal Service provided a list of users with elevated privileges such as super administrator, system administrator, and database administrator.

⁹ These privileged accounts did not have an access request in [REDACTED] or a PS Form [REDACTED].

¹⁰ *Twelve Best Practices for Privileged Access Management*, Gartner, October 8, 2015.

¹¹ Handbook AS-805, *Information Security*, Section 9-3.2.1 Requesting Authorization, May 2015.

¹² Handbook AS-805, Section 6-4.1, General Requirements, and Section 9-6.1.6, Password Expiration.

Management does not adequately monitor privileged accounts.

The Postal Service does not have a comprehensive training program for all privileged users to ensure that they are aware of their roles and responsibilities as well as the risks associated with their elevated privileges.

These issues occurred because management focused on other areas of cyber security and has not yet developed comprehensive guidance for defining, identifying, and managing privileged accounts. System owners also did not require all privileged users to follow Postal Service policy when requesting privileged access and did not ensure that users had an appropriate security clearance prior to issuing access. Further, system owners were not aware of the [REDACTED]. Without proper management of privileged accounts, the Postal Service cannot ensure the confidentiality and integrity of its data, which could lead to unauthorized access, data loss, and reduced confidence in the Postal Service brand.¹³

During our audit, the Engineering Systems group took corrective action by obtaining proper authorizations for privileged users or removing them from the [REDACTED] system. Therefore, we are not making a recommendation regarding [REDACTED] authorization or security clearance issues. In addition, the CISO group developed a management instruction to establish a uniformed approach to managing the Postal Service's privileged accounts; however, this policy is in draft and has not been issued.

Monitoring of Privileged Accounts

Management does not adequately monitor privileged accounts. Specifically, the administrators and owners of the three systems we reviewed and the CISO group are not monitoring the activities of the privileged users on each system. In addition, system administrators and owners do not maintain all audit logs related to privileged user activities in accordance with policy and [REDACTED] managers do not track all last logon dates for their privileged users to ensure individual accountability.

Industry best practices¹⁴ recommend that organizations monitor and reconcile all privileged access activity through system and application logs and Privileged Access Management (PAM) tools. Postal Service policy¹⁵ states that system and database administrators are responsible for ensuring audit logs are implemented and monitored. Postal Service policy¹⁶ also states that management should have the capability to identify users each time they attempt to log on to the system.

This occurred because the Postal Service did not define business practices or responsibilities for monitoring privileged accounts or implement PAM tools in accordance with best practices, require system administrators to follow its policy regarding maintaining audit logs, and did not ensure the [REDACTED] configurations that were inherited from the prior [REDACTED] system complied with current policy. Without proper monitoring of privileged accounts, the Postal Service cannot ensure privileged users have accountability in order to prevent accidental harm or malicious activity. In addition, the Postal Service is at a higher risk of not detecting a cyber intrusion, which could lead to data loss.

Comprehensive Training Program

The Postal Service does not have a comprehensive training program for all privileged users to ensure that they are aware of their roles and responsibilities as well as the risks associated with their elevated privileges. The CISO group developed a training program for all Postal Service domain administrators (Tier 0) on performing administrative functions and identifying practices that put their organization at risk of a compromise. However, no training courses are available to instruct server, application, database

13 [REDACTED]

14 *Twelve Best Practices for Privileged Access Management.*

15 Handbook AS-805, Section 2-2.31, System and Network Administrators, and Section 2-2.32, Database Administrators.

16 Handbook AS-805, Section 9-4.1.3, Individual Accountability.

(Tier 1), and workstation administrators (Tier 2) on how to perform their administrative functions or ensure they are aware of the risks associated with their responsibilities.

Best practices¹⁷ require privileged users to complete security awareness training, role-based training, and specialized training; and acknowledge they understand the responsibilities of their job.

This lack of a comprehensive training program occurred because Postal Service policy¹⁸ and the Strategic Training Initiative (STI)¹⁹ do not require all privileged users to complete privileged user training. Without a comprehensive training program for all privileged users, the Postal Service is at an increased risk of exposure to credential or password compromise, [REDACTED]

[REDACTED].

17 Departments of Defense and Health and Human Services.

18 Handbook AS-805.

19 The STI identifies an employee's required training for the year.

Recommendations

We recommend management develop and continuously maintain a complete and accurate listing of privileged accounts for Postal Service systems.

We recommend the acting chief information security officer and vice president, Digital Solutions:

1. Continue to develop overarching guidance and controls for managing privileged accounts to include establishing a consistent method for identifying all privileged accounts.

We recommend the vice president, Information Technology, in coordination with the acting chief information security office and vice president, Digital Solutions:

2. Develop and continuously maintain a complete and accurate listing of privileged accounts for Postal Service systems.
3. Define business practices and responsibilities for monitoring privileged accounts and implement privileged access management tools.
4. Require administrators for the [REDACTED] and [REDACTED] to follow Handbook AS-805, *Information Security*, regarding maintaining audit logs for privileged users.
5. Develop a comprehensive privileged user training program and update Handbook AS-805, *Information Security*, and the Strategic Training Initiative to require all privileged users to complete the training prior to assuming their privileged role, followed by periodic refresher training.

We recommend the vice president, Engineering Systems:

6. Require administrators for the [REDACTED] to follow Handbook AS-805, *Information Security*, regarding maintaining audit logs for privileged users.

We recommend the senior vice president, Sales and Customer Relations, in coordination the vice president, Information Technology, direct managers, to:

7. Require all users to follow Handbook AS-805, *Information Security*, when requesting and granting privileged access to the [REDACTED] system.
8. Ensure all privileged users have the proper security clearance prior to accessing the [REDACTED] system.

We recommend the vice president, Information Technology, direct the manager, Contact Center Technology, and the vice president, Engineering Systems, direct the manager, Engineering Software Management, to:

9. Establish [REDACTED] settings for privileged accounts to [REDACTED] for the [REDACTED] and [REDACTED] systems.

We recommend the vice president, Information Technology, direct the manager, Contact Center Technology, to:

10. Track last logon settings for the [REDACTED] system.

Management's Comments

Management generally agreed with all of the findings and recommendations in the report and stated that they have begun to take corrective actions. The Postal Service responded that management prioritizes the governance, monitoring, and control of privileged identity management for its SOX and PCI environments and that non-PCI and non-SOX accounts have been on the Postal Service's roadmap for improved Privileged Access Management.

Regarding recommendation 1, the CISO developed a PAM instruction that establishes a procedure for identifying, reviewing, and approving all privileged accounts. The instruction is scheduled for publication by April 30, 2017.

Regarding recommendation 2, the upcoming PAM instruction will require all information resources register in the Access Management and Reporting tool during the Certification and Accreditation process. In addition, system owners and the ISSO will be required to review privileged account access on a quarterly basis. The Postal Service will also be able to develop and continuously maintain a listing of privileged accounts through the Access Management and Reporting tools. Management plans to complete this by June 30, 2018.

Regarding recommendation 3, the upcoming management instruction will require system owners to identify all privileged accounts as part of registering a system in the Access Management and Reporting tools. Monitoring account status will include the account approval process, as well as mandatory periodic manager reviews of privileged accounts. The CISO also plans to implement a PAM solution as part of an overall Identity and Access Management (IAM) transformation. The CISO has begun a current state assessment of the IAM ecosystem at the Postal Service to include the use of privileged accounts. The Postal Service will also be implementing user behavior analytic tools to provide proper monitoring. Management plans to complete this by September 30, 2018.

Regarding recommendation 4, management has begun to take corrective action for these systems to enable audit logging of privileged user access. Management will also have the system administrators follow Handbook AS-805 with regard to maintaining audit logs for privileged users. Management plans to complete this by September 30, 2017.

Regarding recommendation 5, management is in the process of establishing a comprehensive training program for Tier 1, which includes server, application, and database administrators. Management plans to complete this by June 30, 2017.

Regarding recommendation 6, the █████ system currently maintains audit logs for all user accounts, including privileged user accounts. Management stated this was demonstrated to the audit team during the audit process and requests closing this recommendation upon issuance of the report.

Regarding recommendation 7, users will be directed to Handbook AS-805 and the Privileged Access Management Instruction prior to requesting access to privileged roles to the system. In addition, the Postal Service has taken corrective action to approve users with privileged access and is in the process of registering the resources and roles in the Access Management and Reporting tool. Management plans to complete this by September 30, 2017.

Regarding recommendation 8, management stated they took corrective action to ensure privileged users have the proper security clearance prior to the issuance of the final audit report.

Regarding recommendation 9, management took correction action for one of the two systems prior to issuance of the final report and will transfer the other system into a new account that automatically enforces password changes to the proper settings. Management plans to complete this by September 30, 2017.

Regarding recommendation 10, management stated they took corrective action to track privileged users' last logon settings for the referenced systems prior to issuance of the final report.

See [Appendix B](#) for management's comments in their entirety.

Evaluation of Management's Comments

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

Regarding management's comments about the findings, the Postal Service stated that it understands the intent of the report is to help improve the overall posture and capabilities of the Postal Service to enhance cybersecurity processes. Postal Service management also stated that they hold that the findings outlined in the report do not reflect the current state of the enterprise's capabilities or accurately convey the initiatives and measures in progress that will enhance the PAM process.

While the OIG commends management's efforts underway — including development of the PAM instruction, an effort to implement a PAM tool, and participation in the Department of Homeland Security's Continuous Diagnostics and Mitigation program — these efforts have not been fully implemented to date.

Concerning recommendation 6, management stated that during the audit process they demonstrated to the audit team that the [REDACTED] system currently maintains audit logs for all user accounts, including privileged user accounts. The audit team did not receive the audit log information for all [REDACTED] privileged users; however, on March 27, 2017, Postal Service management provided written documentation that the audit logging for GTC is turned on. Therefore, we are closing this recommendation upon issuance of the report.

Regarding recommendations 8 and 10, the Postal Service will need to provide support that it has ensured that privileged users have the proper security clearances and that they are currently tracking last logon settings for the referenced systems before we can close these recommendations.

All recommendations require OIG concurrence before closure. Consequently, the OIG requests written confirmation when corrective actions are completed. Recommendations 1, 2, 3, 4, 5, 7, 8, 9, and 10 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	15
Background	15
Objective, Scope, and Methodology	15
Prior Audit Coverage	16
Appendix B: Management's Comments.....	17

Appendix A: Additional Information

Background

The Postal Service manages access to information resources using multiple types of accounts, including privileged accounts. Privileged accounts are those that have higher levels of rights such as account creation, update and deletion, or full application functionality. Privileged accounts include roles such as domain, system, or database administrator.

The Postal Service uses both automated and manual processes to manage account access and authorization to information resources. The Postal Service uses the [REDACTED] application to manage authorization to most information resources. This application centralizes the management of personnel and machine identities and access rights over the entire life cycle, from account creation to termination.

To establish a privileged user account, personnel must request access via [REDACTED] and receive approval from their manager. If access to an information resource or an account cannot be requested through [REDACTED], then PS Form [REDACTED] (a manual access approval form) must be used. In addition, the Inspection Service uses the [REDACTED] application to request access to resources on the Inspection Service domain.

It is important that privileged accounts be established in a manner that ensures access is granted based on least privileges required for the user to perform their duties, separation of duties, and security clearance requirements. Proper management and assignment of privileged accounts help prevent breaches and insider attacks. [REDACTED]

Best practices recommend organizations use PAM tools to properly manage privileged accounts. PAM tools help secure, manage, and monitor privileged accounts and activities within an organization, helping to ensure the confidentiality of information and reduce the risk of unauthorized modifications to systems and data.

Objective, Scope, and Methodology

Our objective was to determine if the Postal Service is effectively managing privileged accounts in accordance with Postal Service policy and best practices. The scope of this audit was all Postal Service privileged accounts.

To accomplish our objective, we:

- Researched Postal Service and best practices policies and procedures related to managing and monitoring privileged accounts and training privileged account users.
- Reviewed how the Postal Service manages and monitors privileged accounts throughout the organization.
- Reviewed privileged user training courses and compared them to best practices.
- Obtained and reviewed partial listings of privileged accounts.

Since the Postal Service did not have processes in place to identify a complete universe of all privileged accounts, we obtained a complete listing of over [REDACTED] systems in the [REDACTED]⁰ to judgmentally select three high criticality systems for further review. The three systems were [REDACTED], and [REDACTED]. The three critical systems selected were non-PCI-DSS and non-SOX systems. PCI-DSS is a widely accepted set of policies and procedures intended to optimize the security of credit, debit, and cash card transactions and protect cardholders against misuse of their personal information. SOX is a federal law protecting investors from the possibility of fraudulent accounting activities by corporations and requiring management to certify the accuracy of their reported financial statements.

For each system we:

- Determined how the Postal Service managed access to privileged accounts including the approval and deactivation process.
- Requested and reviewed a list of privileged accounts to determine if the account was properly requested and managed, if the user had the appropriate security clearance, and if the account [REDACTED].
- Determined how the Postal Service monitored privileged accounts including whether they maintained system and audit logs.
- Reviewed privileged user training.

We conducted this performance audit from September 2016 through April 2017, 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 February 22, 2017 and included their comments where appropriate.

We assessed the reliability of privileged account user data by observing the data being extracted by system administrators. We determined that the data were sufficiently reliable for the purposes of this report.

Prior Audit Coverage

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

²⁰ The Postal Service's database of record that maintains information about existing applications, tool sets, and data.

Appendix B: Management's Comments



March 21, 2017

Lori Lau Dillard
Director, Audit Operations

SUBJECT: Response to Draft Report: Privileged Account Management
(IT-AR-17-DRAFT) Project Number 16TG021IT000

Thank you for the opportunity to respond to the Privileged Account Management (PAM) audit report. Cybersecurity remains a top priority across the Postal Service, as demonstrated by management's implementation of a robust, multi-year transformation program. As we continue to modernize our information security framework, the focus of the ongoing transformation efforts is to better protect customers, employees, and the enterprise from present-day and future threats. Accordingly, the PAM audit represents an important component of a larger USPS cybersecurity strategy.

Management understands the intent of the draft report is to help improve the overall posture and capabilities of the Postal Service to enhance cybersecurity processes. However, management holds that the findings outlined in this report do not reflect the current state of the enterprise's capabilities or accurately convey the initiatives and measures in progress that will enhance the Privileged Account Management process. The Privileged Account Management governance structure, monitoring procedures, and oversight policies are pending substantial upgrades upon the issuance of a Management Instruction (MI) developed prior to the initiation of this audit. As such, while we generally agree with the intent of the findings, we believe the Postal Service has established robust processes to manage privileged accounts effectively.

Prior to the initiation of the PAM audit, the Postal Service already instituted several measures to both strengthen and maintain the effectiveness of controls over privileged accounts. Numerous steps have been taken since FY2015 to address privileged account management including the following:

1. In 2015, management established Initiative #13 (Identity and Access Management). This effort devotes considerable resources to setting policies and guidelines for managing privileged access.

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

2. The Postal Service prioritized governance, monitoring, and control procedures of privileged identity management for its Sarbanes-Oxley Act (SOX) and Payment Card Industry (PCI) environments to address the SOX Significant Deficiency and other specific issues regarding access management.
3. Due to their criticality, SOX and PCI were treated with greater urgency. Non PCI/SOX accounts have been on the Postal Service roadmap for improved PAM. For the SOX environment, the Postal Service created a protected administrator domain using a secure privileged information management (PIM) methodology, including user training, special administration workstations, smart cards, and two-factor authentication to safeguard systems. Routine penetration testing further monitors compliance with cybersecurity policies and processes.
4. Management prepared a Management Instruction to initiate new policies that strengthen monitoring procedures for privileged accounts. The MI calls for automating the information resource registration process, enabling greater administration and oversight of privileged account users.
5. In February 2017, CISO released a RFI to numerous IAM vendors to obtain information on a range of products to include PAM tools. This is an effort to implement a PAM solution as part of an overall Identity and Access Management transformation across the variety of complex operating environments that make up the USPS infrastructure.
6. The Postal Service participates in the Department of Homeland Security's Continuous Diagnostics and Mitigation (CDM) program. The CDM provides agencies with leading PIM solutions. Management will continue to support the initiative and further investment in leading PIM technologies on the project timeline for the privileged account management work into FY2018. The Postal Service participation in CDM underscores its strong alignment with U.S. governments program around privileged account management.

The Postal Service understands the risks associated with privileged accounts and has taken many proactive steps to promote authorized access to systems. Management looks forward to working in partnership with the Postal Service Office of the Inspector General to advance leading practices throughout the enterprise.

Recommendation [1]:

Continue to develop overarching guidance and controls for managing privileged accounts to include establishing a consistent method for identifying all privileged accounts.

Management Response/Action Plan:

Management agrees with this recommendation. The Corporate Information Security Office (CISO) developed a Privileged Access Management Instruction that establishes a procedure for identifying, reviewing, and approving all privileged accounts, scheduled for publication in April 2017.

Target Implementation Date:

April 30, 2017

Responsible Official:

Vice President, Chief Information Security Officer

Recommendation [2]:

Develop and continuously maintain a complete and accurate listing of privileged accounts for Postal Service systems.

Management Response/Action Plan:

Management agrees with this recommendation. The forthcoming Privileged Account Management Instruction will require all information resources register in the Access Management and Reporting tool during the Certification and Accreditation process. Also, information system owners and the Information System Security Office assigned to the system will be required to review privileged account access on a quarterly basis. As such, the Postal Service will be able to develop and continuously maintain a listing of privileged accounts through the Access Management and Reporting tools.

Target Implementation Date:

June 30, 2018

Responsible Official:

Vice President, Information Technology
Vice President, Chief Information Security Officer

Recommendation [3]:

Define business practices and responsibilities for monitoring privileged accounts and implement privileged access management tools.

Management Response/Action Plan:

Management agrees with the intent of this recommendation. The upcoming Management Instruction will require system owners to identify all privileged accounts as part of registering a system in the Access Management and Reporting tool. The account approval process, as well as mandatory periodic manager reviews of privileged accounts, monitor account status.

CISO plans to implement a Privileged Account Management (PAM) solution, as part of an overall Identity and Access Management (IAM) transformation. To prepare for such implementation, CISO has begun a current state assessment of the IAM ecosystem at USPS, to include use of privileged accounts. This assessment will identify key requirements and use cases for a PAM solution. In addition, the Postal Service will be implementing user behavior analytics tools to provide proper monitoring.

Target Implementation Date:

September 30, 2018

Responsible Official:

Vice President, Information Technology
Vice President, Chief Information Security Officer

Recommendation [4]:

Require administrators for the [REDACTED] and [REDACTED] System to follow Handbook AS-805, Information Security, regarding maintaining audit logs for privileged users.

Management Response/Action Plan:

Management agrees with this recommendation. Corrective actions have been taken for these systems to enable audit logging of privileged user access prior to the issuance of the final report. Additionally, management will have the administrators for these systems to follow Handbook AS-805 in regards to maintaining audit logs for privileged users.

Target Implementation Date:

September 30, 2017

Responsible Official:

Vice President, Information Technology
Vice President, Chief Information Security Officer

Recommendation [5]:

Develop a comprehensive privileged user training program and update Handbook AS-805, Information Security, and the Strategic Training Initiative to require all privileged users to complete the training prior to assuming their privileged role, followed by periodic refresher training.

Management Response/Action Plan:

Management agrees with the intent of this recommendation. A training program is currently in place for Tier 0, and management is in the process of establishing a comprehensive training program for Tier 1, which includes server, application, and database administrators. The privileged user training guidelines are addressed using different standards.

Target Implementation Date:

June 30, 2017

Responsible Official:

Vice President, Information Technology
Vice President, Chief Information Security Officer

Recommendation [6]:

Require administrators for the [REDACTED] to follow Handbook AS-805, Information Security, regarding maintaining audit logs for privileged users.

Management Response/Action Plan:

Management agrees with this recommendation. The [REDACTED] system currently maintains audit logs for all user accounts, including privileged user accounts. This was demonstrated to the audit team during the audit process.

Target Implementation Date:

Management recommends closing this recommendation.

Responsible Official:

Vice President, Engineering Systems

Recommendation [7]:

Require all users to follow Handbook AS-805, Information Security, when requesting and granting privileged access to the [REDACTED] system.

Management Response/Action Plan:

Management agrees with the intent of this recommendation. Users will be directed to AS-805 and the Privileged Access Management Instruction prior to requesting access to privileged roles to the system. Additionally, the system has taken corrective action to approve users with privileged access and is in the process of registering the resources and roles in the Access Management and Reporting tool.

Target Implementation Date:

September 30, 2017

Responsible Official:

Senior Vice President, Sales and Customer Relations
Vice President, Information Technology

Recommendation [8]:

Ensure all privileged users have the proper security clearance prior to accessing the [REDACTED] system.

Management Response/Action Plan:

Management agrees with this recommendation and has taken corrective actions to ensure privileged users have proper security clearance, prior to the issuance of the final PAM audit report.

Target Implementation Date:

March 30, 2017

Responsible Official:

Senior Vice President, Sales and Customer Relations
Vice President, Information Technology

Recommendation [9]:

Establish [REDACTED] for the [REDACTED] and [REDACTED] systems.

Management Response/Action Plan:

Management agrees with the intent of this recommendation and took corrective actions for one of the two systems referenced above prior to the issuance of the final report. The other system will be transferred into a new account that will automatically enforce [REDACTED] to the above settings.

Target Implementation Date
September 30, 2017

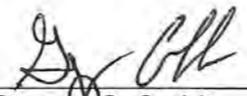
Responsible Official:
Vice President, Information Technology
Vice President, Engineering Systems

Recommendation [10]:
Track last logon settings for the [REDACTED] system.

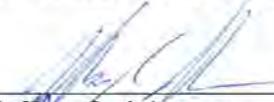
Management Response/Action Plan:
Management agrees with this recommendation and has taken corrective actions to track last logon settings for the referenced systems privileged users prior to the issuance of the final report.

Target Implementation Date
March 30, 2017

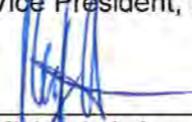
Responsible Official:
Vice President, Information Technology



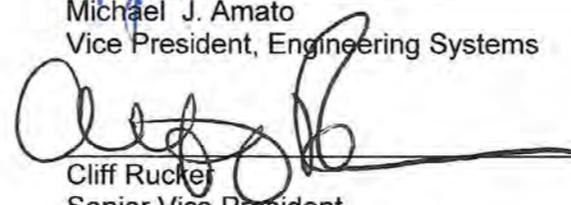
Gregory S. Crabb
Vice President, Chief Information Security Officer



Jeffrey C. Johnson
Vice President, Information Technology



Michael J. Amato
Vice President, Engineering Systems



Cliff Rucker
Senior Vice President
Sales and Customer Relations

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