OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

Review of Selected Active Directory Domains

Audit Report

Report Number
IT-AR-16-006

February 10, 2016

OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

Highlights

Postal Service management did not appropriately configure and manage the five domains we reviewed on the IT network.

Background

The U.S. Postal Service uses Microsoft's Active Directory (AD) to control access to more than 192,000 information resources managed by 183 domains on the Postal Service information technology (IT) network. Users can access systems and services through AD once they enter a user name and password.

Administrators use AD to set up and manage user accounts, computers, policies, and permissions. Within AD, domains manage user accounts, including groups of users and computers with similar requirements. Effective management of AD allows organizations to adequately secure and protect critical information resources from accidental or intentional unauthorized use.

Fifteen AD domains manage the majority of the Postal Service IT network. Management reviews these domains periodically to comply with the Sarbanes-Oxley Act and Payment Card Industry Data Security Standards. We judgmentally selected and analyzed five of the 168 domains that are not regularly reviewed. We chose these five domains because they support a large number of servers and workstations.

Our objective was to determine whether selected domains were configured and managed in accordance with policy and industry best practices.

What the OIG Found

Postal Service management did not appropriately configure and manage the five domains we reviewed. We found that up to 40 percent of the security settings we reviewed for each domain did not fully comply with Postal Service security standards. In addition, we found 15 of 75 security settings within AD (20 percent) were not consistent with Microsoft's best practices. For example, we determined the Postal Service [redacted] security standard has a "maximum password age" of [redacted] days, while Microsoft recommends a "maximum password age" of 30 to 90 days to ensure an attacker has limited time to crack a password.

Management also did not appropriately manage privileged accounts for three of the five domains we reviewed. Specifically, two shared administrator accounts existed on one domain and two [redacted] accounts on two domains were [redacted] required by policy. Further, management allowed administrators for three of the five domains to use accounts with [redacted] and did not require domain administrators for four of the five domains to change account passwords at least every 30 days as required by policy.

The domains were not properly configured because administrators were unaware of the applicable Postal Service security standards or did not have access to them.

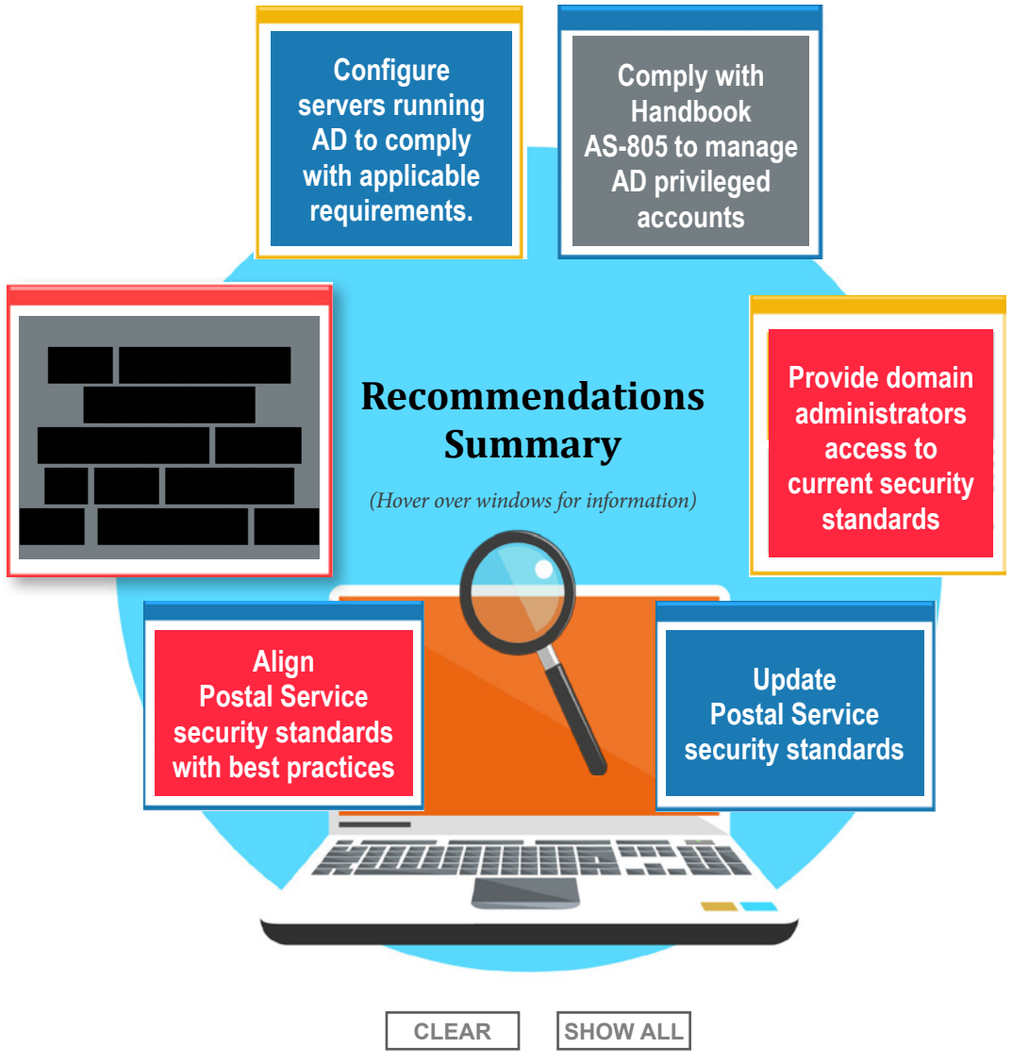
OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

Administrators also did not have a schedule to periodically review the standards to ensure compliance.

Without the proper security controls and requirements over domains, the Postal Service is at an increased risk of unauthorized users gaining access to its resources.

What the OIG Recommended

We recommended management provide domain administrators access to current security standards and ensure administrators configure servers running AD to comply with applicable requirements. We also recommended domain administrators comply with Handbook AS-805, *Information Security*, to manage AD privileged accounts, including [redacted], removing accounts [redacted], and changing administrative account passwords. Finally, we recommended the Corporate Information Security Office update Postal Service security standards and align them with best practices where appropriate.



Transmittal Letter

OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

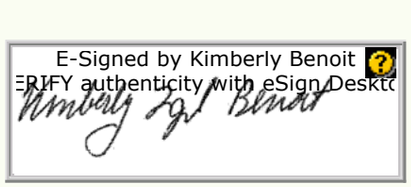
February 10, 2016

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

MICHAEL J. AMATO
VICE PRESIDENT, ENGINEERING SYSTEMS

LINDA M. MALONE
VICE PRESIDENT, NETWORK OPERATIONS

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



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

SUBJECT: Audit Report – Review of Selected Active Directory Domains
(Report Number IT-AR-16-006)

This report presents the results of our audit of the U.S. Postal Service's Review of Selected Active Directory Domains (Project Number 15TG034IT000).

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 and Response Management

Table of Contents

Findings

Domain administrators did not appropriately configure and manage the [redacted] domain controllers we reviewed as required by policy.

Introduction

This report presents the results of our self-initiated audit of selected U.S. Postal Service Active Directory Domains (Project Number 15TG034IT000). Our objective was to determine whether selected domains were configured and managed in accordance with policy and industry best practices. See Appendix A for additional information about this audit.

The Postal Service uses Microsoft's Active Directory (AD) to control access to more than 192,000 information resources on the Postal Service's information technology (IT) network. AD is a centralized system that allows domain administrators[1] to manage user accounts, computers, policies, and permissions. Users can access systems and services through AD once they authenticate with the proper user name and password. Within AD, domains manage user accounts, including managing groups of users and computers by setting similar policies and providing access to network resources within each domain. Domain controllers are servers running AD services that support a domain.

Summary

Postal Service management did not appropriately configure and manage the five domains we reviewed[2] on the IT network. We found that up to 40 percent of the security settings we reviewed for each domain did not fully comply with Postal Service security standards. In addition, the Corporate Information Security Office (CISO) did not fully align Postal Service security standards with Microsoft's best practices and management did not appropriately manage privileged accounts for three of the five domains by having two shared administrator accounts and not [redacted] privileged accounts. In addition, [redacted] was not set for three of the five domains and there was no requirement to change administrative account passwords every 30 days for four of the five domains.

These issues occurred because administrators were unaware of applicable Postal Service security standards or did not have access to them and did not have a schedule to review standards periodically to ensure compliance. Management also did not make it a priority to update [redacted] server security standards to align with best practices and be consistent with Postal Service security standards found in Handbook AS-805.[3] By implementing effective management over AD, organizations can appropriately secure their information resources and reduce the risk of attackers exploiting vulnerable services and settings.

Management of Domain Controllers

Domain administrators did not appropriately configure and manage the [redacted] domain controllers[4] we reviewed as required by policy.[5] We found that they were not fully compliant with Postal Service security standards related to configuration settings and system service settings.

---

1 Postal Service personnel who are assigned administrative accounts with higher level access rights for domain management including account creation, update, and deletion.
2 We conducted our audit work on the [redacted] domains at Postal Service facilities in Merrifield, VA; Norman, OK; and Topeka, KS; and the [redacted] domain in Chantilly, VA.
3 Handbook AS-805, *Information Security*, May 2015.
4 We judgmentally selected and tested 5 of the168 domains that are not required to follow Sarbanes-Oxley (SOX) and Payment Card Industry Data Security Standards (PCI DSS) based on the highest number of systems they support. We reviewed the [redacted] domains and the [redacted] associated domain controllers.
5 Handbook AS-805, Section 10-2.3.1, Hardening Servers; and Section 11-3.6, Implementing Hardening Standards.

Configuration settings define the way a computer system or program is set up for a particular use. The non-compliant configuration settings we identified included [redacted] These configuration settings track and log system changes that management can review in the future.

System service settings are programs that load automatically to support the system's various tasks. These settings can be part of an application's startup process or an operating system's startup process. We found that two system service settings were noncompliant: [redacted] service was disabled and [redacted][1] service was not installed. These system services are critical for blocking unauthorized network traffic and detecting and removing malware.[12]

Table 1 shows the number of configuration and system service settings that were not compliant with Postal Service standards for the five domains we tested.[13]

Table 1. Compliance With Postal Service Security Settings by Domain

Domain[14]	Domain Controller Name	Number of Configuration Settings not Compliant with Postal Service Standards	Percentage not Compliant with Postal Service Standards	Number of System Service Settings not Compliant with Postal Service Standards	Percentage not Compliant with Postal Service Standards
[redacted]	[redacted]	14	29%	7	23%
	[redacted]	14	29%	6	20%
	[redacted]	12	24%	1	6%
[redacted]	[redacted]	11	22%	1	6%
	[redacted]	11	22%	1	6%
[redacted]	[redacted]	25	33%	5	17%
	[redacted]	25	33%	12	40%
[redacted]	[redacted]	29	39%	6	20%
	[redacted]	29	39%	6	20%
[redacted]	[redacted]	27	36%	5	17%
	[redacted]	27	36%	5	17%
	[redacted]	27	36%	5	17%

Source: U.S. Postal Service Office of Inspector General (OIG) results of automated scripts.

6 This security setting determines whether the system logs [redacted].
7 This security setting determines whether the system logs [redacted]
8 This security setting determines whether the system logs [redacted] It has its own system access control list specified.
9 This security setting determines whether the operating system [redacted]
10 This service helps protect your computer by [redacted]
12 Malicious software designed to gain access or damage a computer without the knowledge of the owner. There are various types of malware including spyware, keyloggers, viruses, worms, or any type of malicious code that infiltrates a computer.
13 We reviewed 49 configuration settings and 17 system service settings in the Postal Service [redacted] server security standard. We also reviewed 75 configuration settings and 30 system service settings in the Postal Service [redacted] server security standard.
14 See Appendix A for a description of the five domains we selected.
15 This domain did not have group policy established for some of the configuration settings and local policy was the default setting; therefore, the three [redacted] domain controllers had slight differences in their settings.

Administrators did not configure domain controller security settings appropriately because they were unaware of applicable Postal Service security standards or did not have access to them. In addition, administrators did not have a schedule for periodically reviewing the standards to ensure compliance. Without proper controls and requirements over the domains, the Postal Service is at an increased risk of unauthorized users gaining access to Postal Service resources.

During our audit, management initiated corrective action by updating the configurations of two of the five domains we reviewed.[16] However, corrective action is needed to address the remaining non-compliant configurations.

Alignment with Best Practices

CISO did not fully align Postal Service security standards with Microsoft's best practices in some instances. We identified security settings on five of 49 [redacted] servers (10 percent) and 15 of 75 [redacted] servers (20 percent) that were not consistent with Microsoft's best practices. For example:

- Postal Service [redacted] server security standards have a "maximum password age" of [redacted] days; however, Microsoft recommends a "maximum password age" of between 30 and 90 days to limit the time an attacker has to crack a password and access network resources.

- Postal Service [redacted] server security standards have a "minimum password age" of [redacted] days; however, Microsoft recommends a "minimum password age" of two days to ensure users cannot continue to change passwords repeatedly until they reach a favorite old password.

- Postal Service [redacted] server security standards have the [redacted] set to [redacted]. However, Microsoft recommends enabling this function to ensure attackers cannot access [redacted].

In addition, we identified inconsistencies between Postal Service security standards for [redacted] servers and Handbook AS-805's requirement for the "maximum password age." Handbook AS-805 requires administrators to change their passwords at least every 30 days and all other user accounts at least every 90 days; however, Postal Service security standards for [redacted] servers require a "maximum password age" of [redacted] days.

These issues occurred because management did not make it a priority to update [redacted] server security standards to align with best practices and ensure consistency with Handbook AS-805. The SysAdmin, Audit, Networking, and Security (SANS) Institute[17] recommends that organizations establish, actively manage, and correct the security configuration of laptops, servers, and workstations to prevent attackers from exploiting vulnerable services and settings. These configurations should be continually managed to account for new security vulnerabilities and support new operational requirements. By including industry best practices in security standards, organizations are better prepared to identify risks to their environment and incorporate changes needed to meet their business objectives.

---

16 Three [redacted] domain controller settings were changed to comply with Postal Service security standards as follows: [redacted] changed eight of 14 non-compliant configuration settings and six of seven system service settings; [redacted] changed eight of 14 non-compliant configuration settings and five of six system service settings; and [redacted] changed six of 12 non-compliant configuration settings. In addition, two [redacted] domain controllers were changed to comply with Postal Service security standards through installation of [redacted].

17 The SANS Institute develops, maintains, and makes available, at no cost, the largest collection of research documents about various aspects of information security.

Postal Service management did not appropriately manage administrative accounts for three of the five domains we reviewed.

Administrative Accounts

Postal Service management did not appropriately manage administrative accounts[18] for three of the five domains we reviewed. For example, one domain[19] used two shared administrative accounts to manage the entire domain instead of establishing individual administrative accounts.[20] In addition, domain administrators did not [redacted] for two domains[21] that had been [redacted] days as required by policy.[22] As a best practice,[23] Microsoft recommends disabling the default administrator account in each domain.

Domain administrators did not properly manage these accounts because they were not familiar with Handbook AS-805 requirements for administrative accounts. When administrative accounts are not secure, an attacker can obtain administrative access to a domain controller to modify, corrupt, and destroy the AD database and all systems and accounts AD manages.

Password Expiration

Postal Service management did not ensure proper controls over password expiration were in place. We found that administrative accounts were set to have passwords [redacted]. Administrators also did not change administrative account passwords[24] at least every 30 days as required by policy.[25] We identified administrative accounts with passwords that do not expire for three of the five domains we reviewed. In addition, four of the five domains had accounts with passwords ranging from [redacted]

Table 2 shows the administrative accounts not compliant with Postal Service policy.[26]

Table 2. Administrative Account Compliance by Domain

Domain	Number of Administrative Accounts	Administrative Accounts with Passwords that do not Expire	Administrative Accounts with Passwords Over 30 Days Old
[redacted]	7	3	4
[redacted]	6	0	2
[redacted]	2	0	0
[redacted]	7	1	5
[redacted]	19	4	9

Source: According to data provided by Postal Service domain administrators.

AD administrators did not follow password requirements because they were not familiar with the Handbook AS-805 policy for managing administrative accounts. If appropriate password protocols are not followed, information resources may be at risk of compromise and disclosure of sensitive information.

18 Privileged or administrative accounts are protected accounts with higher level access rights for domain management including account creation, update, and deletion.
19 The [redacted] domain used two shared administrator accounts to manage the domain.
20 Handbook AS-805, Section 9-4.2.4, Shared Accounts.
21 The [redacted] and [redacted] domains had an administrative account that was [redacted] and was not disabled as required by policy.
22 Handbook AS-805, Section 9-4.3, Account Management.
23 *Microsoft Best Practices for Securing AD*, Appendix D, [redacted]
24 Passwords are unique strings of characters that personnel or information resources provide in conjunction with a log-on ID to gain access to an information resource.
25 Handbook AS-805, Section 9-6.1.6, Password Expiration; and Section 9-6.1.7, Request for Use of Nonexpiring Password Accounts.
26 Handbook AS-805, Section 9-6.1.6, Password Expiration; and Section 9-6.1.7, Request for Use of Nonexpiring Password Accounts.

During our audit, management initiated corrective action by changing the security settings on one administrative account so the password would expire; however, corrective action is still needed to address administrative account discrepancies on all five domains.

Recommendations

We recommend management provide domain administrators access to current security standards and direct domain administrators to comply with Handbook AS-805, Information Security, to manage Active Directory administrative accounts, including [redacted] and are not approved by management, and changing administrative account passwords.

We recommend the acting vice president, Information Technology, coordinate with the vice president, Engineering Systems, and vice president, Network Operations, to:

1. Provide domain administrators access to current security standards.

2. Direct domain administrators to configure servers running Active Directory to meet requirements outlined in applicable Postal Service security standards.

3. Direct domain administrators to comply with Handbook AS-805, *Information Security*, to manage Active Directory administrative accounts, including [redacted] and are not approved by management, and changing administrative account passwords.

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

4. Update current [redacted] server security standards and align them with best practices where appropriate to enhance the overall security of Active Directory.

Management's Comments

Management agreed with the findings and recommendations 1 through 3 and partially agreed with recommendation 4. See Appendix B for management's comments in their entirety.

Regarding recommendation 1, management stated they have already provided domain administrators access to appropriate security standards and will continue to provide administrators with access to the current standards. The target implementation date is February 29, 2016. Management requested closure of this recommendation with the issuance of the report.

Regarding recommendations 2 and 3, management stated they will direct domain administrators to configure servers running AD to meet the requirements outlined in applicable Postal Service security standards. In addition, management will direct domain administrators to comply with appropriate Handbook AS-805 standards. Management also stated they have begun a large-scale initiative to appropriately configure all AD domains. The target implementation date is July 31, 2016.

Regarding recommendation 4, management stated they will update [redacted] server security standards but disagrees with the recommendation to update [redacted] security standards since [redacted] is at end-of-life. Management stated they are evaluating options for migrating these servers to a supported operating system or document appropriate risk acceptance. The target implementation date is July 31, 2016.

Evaluation of Management's Comments

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

Regarding recommendation 1, management requests closure of this recommendation with the issuance of the final report. However, the OIG will not close out the recommendation until we receive support that management has provided domain administrators with the appropriate security standards.

Regarding recommendation 4, the OIG agrees that migrating the [redacted] servers to a supported operating system or performing an analysis to determine if the risk would be acceptable to the Postal Service would be an appropriate alternative solution.

All recommendations require OIG concurrence before closure. Consequently, the OIG requests written confirmation when corrective actions are completed. These recommendations should not be closed in the Postal Service's follow-up tracking system until the OIG provides written confirmation that the recommendations can be closed.

Appendices

Click on the appendix title to the right to navigate to the section content.

Appendix A: Additional Information

Background

The Postal Service has about 183 AD domains enterprise-wide on its IT network. The majority of Postal Service information resources are centrally managed by 15 domains, including the [redacted] domain,[27] which must follow SOX[28] and PCI DSS[29] and undergo an annual review by designated groups.[30] However, about 168 domains are not required to follow SOX and PCI requirements and are not reviewed annually. These domains pose a risk to the network if the Postal Service does not manage and appropriately secure them. By implementing appropriate security controls and management practices for the entire environment, the Postal Service is better prepared to defend its data and systems against emerging threats and potential unauthorized access.

We reviewed five domains presenting a risk to the Postal Service based on their support of about 1,153 servers and workstations. These domains protect Postal Service data on the IT network. Specifically:

- [redacted] domain controllers at the Central Repair Facility in Topeka, KS, protect information on file servers about equipment repairs, historical data for repair items, and sensitive proprietary information regarding technical designs for privately owned equipment used to develop test procedures and make equipment repairs.
- [redacted] domain controllers at Engineering Systems Headquarters (HQ) in Merrifield, VA, protect information supporting file and print servers and administrative data.
- [redacted] domain controllers at the [redacted] business partner site in Chantilly, VA, protect code data and information for developing, managing, and operating about 51 Postal Service applications, including [redacted] and [redacted].
- [redacted] domain controllers at Engineering Systems HQ in Merrifield, VA, protect the mail processing network within the processing plant to provide visibility of switch configuration data.
- [redacted] domain controllers at Engineering Systems HQ in Merrifield, VA, and Norman, OK, protect mail processing barcode scan information.

Objective, Scope, and Methodology

Our objective was to determine whether selected domains were configured and managed in accordance with policy and industry best practices. We judgmentally selected and tested five of the 168 domains that are not required to follow SOX and PCI DSS requirements based on the highest number of systems they supported. We reviewed the [redacted].

To accomplish our objective, we:

- Performed onsite enumeration scans in July 2015, using Nbtscan[31] to identify all AD domains on the Postal Service IT network. We performed scans at the IT/Accounting Service Center in Eagan, MN, and the Northern Virginia Processing and Distribution

27 Serves as the enterprise-wide service for about 187,000 computers and validates the identity of individuals who request access to about 99 percent of all Postal Service applications.
28 A law enacted to protect shareholders and the general public from accounting errors and fraudulent practices in the enterprise and improve the accuracy of corporate disclosures. The U.S. Securities and Exchange Commission administers the act, which sets deadlines for compliance and publishes rules on requirements.
29 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.
30 Postal Service officials and contracting groups conducted SOX and PCI testing for 2015. The Postal Service IT Compliance Management Office coordinated this testing.
31 A command line tool that scans for Windows devices on a local or remote network.

Center in Merrifield, VA. Our scans identified 183 domains on the Postal Service IT network. We removed 15 domains subject to fiscal year 2015 security control testing by SOX and PCI groups. We judgmentally selected five of 168 remaining domains posing a risk to the Postal Service environment based on their support of the highest number of systems (servers and workstations) for further review.

- Performed onsite testing in August 2015 using automated scripts to collect data on the five domains at the Central Repair Facility, Engineering Systems HQ and the [redacted] business partner site. We obtained data to evaluate group policy security settings, privileged user accounts, access levels, account provisioning, and trust relationships for each domain.

- Analyzed and compared our results to Postal Service security standards and Microsoft best practices to determine if existing security settings were appropriate and in compliance with security standards and identified potential vulnerabilities. We also interviewed appropriate personnel to evaluate current policies and procedures for managing and maintaining selected domains.

We conducted this performance audit from June 2015 through February 2016, in accordance with generally accepted government auditing standards and included such tests of internal controls, as we considered necessary under the circumstances. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. We discussed our observations and conclusions with management on January 11, 2016, and included their comments where appropriate.

We assessed the reliability of computer-generated data by performing automated testing. We assessed the reliability of configuration data on domain controllers by reviewing existing documentation, obtaining additional records, 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

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

Appendix B: Management's Comments

UNITED STATES POSTAL SERVICE

LORI LAU DILLARD
DIRECTOR, AUDIT OPERATIONS

SUBJECT: Response to Draft Report: Review of Selected Active Directory Domains (IT-AR-16-DRAFT), Project Number 15TG034IT000

Thank you for the opportunity to review and comment on the subject draft audit report. Management understands the intent of the draft report is to help improve the overall security posture and capabilities of the Postal Service to defeat and otherwise mitigate cybersecurity risks. Overall, USPS agrees with the findings identified in the report. During the course of the audit, management began to initiate corrective actions to address the specific findings related to the identified domains and to enhance Active Directory domain security. These corrective actions included updating password and administrator account settings for the domains to align with Microsoft best practices.

Protecting the privacy of customer, employee, supplier and Postal Service information has been and always will be a priority for the Postal Service. USPS has developed and is executing an aggressive multi-phased cybersecurity improvement strategy to meet its security objectives and to protect information and assets across the enterprise. As part of this strategy, USPS management has developed a larger plan to address all outstanding security concerns with Active Directory domains. The specific compliance gaps identified by the OIG in this report will be addressed as part of this larger initiative.

Recommendation [1]:
Provide domain administrators access to current security standards.

Management Response/Action Plan:
Management agrees with the recommendation and has already provided domain administrators access to appropriate security standards. Management will continue to provide administrators with access to the current standards and requests closure of this recommendation with the issuance of the final report.

Target Implementation Date:
February 29, 2016

Responsible Official:
Manager, Desktop Computing, Information Technology
Manager, Engineering Software Management, Engineering Systems
Manager, Maintenance Operations, Network Operations

Recommendation [2]:
Direct domain administrators to configure servers running Active Directory to meet requirements outlined in applicable Postal Service security standards.

Management Response/Action Plan:
Management agrees with the recommendation and will direct domain administrators to configure servers running Active Directory to meet the requirements outlined in applicable Postal Service

475 L'ENFANT PLAZA SW
WASHINGTON DC 20260-5000
WWW.USPS.COM

Security Standards. During the course of this audit, USPS teams have already been working to configure the servers appropriately and will continue to update the domains to meet relevant security standards. USPS management has begun a large-scale initiative to address all domains currently running and will continue to address these findings as part of this effort. In order to close this recommendation, USPS management will coordinate with the OIG to run appropriate scripts to demonstrate compliance for the domains.

Target Implementation Date:
July 31, 2016

Responsible Official:
Manager, Desktop Computing, Information Technology
Manager, Engineering Software Management, Engineering Systems
Manager, Maintenance Operations, Network Operations

Recommendation [3]:
Direct domain administrators to comply with Handbook AS-805, *Information Security*, to manage Active Directory administrative accounts, including [redacted] and are not approved by management, and changing administrative account passwords.

Management Response/Action Plan:
Management agrees with the recommendation and will direct domain administrators to comply with the appropriate Handbook AS-805, *Information Security*, standards. During the course of this audit, USPS teams have already been working to configure the servers appropriately and will continue to update the domains to meet all relevant security standards. USPS management has begun a large-scale initiative to address all domains currently running and will continue to address these findings as part of this effort. In order to close this recommendation, USPS management will coordinate with the OIG to run appropriate scripts to demonstrate compliance for the domains.

Target Implementation Date:
July 31, 2016

Responsible Official:
Manager, Desktop Computing, Information Technology
Manager, Engineering Software Management, Engineering Systems
Manager, Maintenance Operations, Network Operations

Recommendation [4]:
Update current [redacted] server security standards and align them with best practices where appropriate to enhance the overall security of Active Directory.

Management Response/Action Plan:
Management partially agrees with the recommendation and will update server security standards for [redacted] to align with best practices where appropriate. Management disagrees with the recommendation to update [redacted] security standards; since [redacted] is at end-of-life, management is currently evaluating options to migrate these servers to a supported operating system or document appropriate risk acceptance.

Target Implementation Date:
July 31, 2016

Responsible Official:
Chief Information Security Officer & Digital Solutions, Vice President

Michael J. Amato
Vice President, Engineering Systems

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

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

Linda M. Malone
Vice President, Network Operations

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