March 24, 2010

ROSS PHILO
EXECUTIVE VICE PRESIDENT AND CHIEF INFORMATION OFFICER

CHARLES L. MCGANN
MANAGER, CORPORATE INFORMATION SECURITY

SUBJECT: Audit Report – Windows Access Controls at the Information Technology and Accounting Service Centers – IS General Controls FY 2009 (Report Number IS-AR-10-006)

This report presents the results of our audit of Windows® access controls [redacted], [redacted] Information Technology and Accounting Service Centers (IT/ASCs) and the Information Technology Service Center (ITSC) [redacted] (Project Number 09RD001IS005). Our objective was to determine whether the U.S. Postal Service established adequate logical controls to limit or detect inappropriate access to its Windows operating environment. We performed this self-initiated review as part of the fiscal year (FY) 2009 information systems audit of general controls. See Appendix A for additional information about this audit.

Conclusion

The Postal Service established adequate logical controls to limit or detect inappropriate access to its Windows operating environment [redacted]. However, management can improve access controls by regularly maintaining Active Directory®[1] objects and complying with Windows security standards.

Active Directory Management

System administrators were not updating the Active Directory Organizational Units (OUs), groups, and accounts [redacted] as required by Windows security standards and Postal Service policy.[2] This occurred because administrators do not have clearly defined responsibilities for maintaining and regularly updating Active Directory objects. By properly maintaining and updating Active Directory objects, management can reduce the risk of unauthorized access to Postal Service information resources, access authority exceeding job responsibilities, and operational disruptions. See Appendix B for our detailed analysis of this topic.

[1] A hierarchical database that stores information about two broad categories of computer objects: resources (e.g., printers, workstations, and servers) and security principals (e.g., user or computer accounts and groups, such as organizational units). Each object has a uniquely assigned security identifier, which controls access and sets security.
[2] *Security Standards for Windows 2003 Servers*, Section 1.2, Purpose, revised March 1, 2009. Handbook AS-805, *Information Security*, Section 9-3.2.5, Periodic Review of Access Authorization.

We recommend the manager, Corporate Information Security, work with the manager, Information Technology Engineering and Architecture, to:

1. Revise the *Security Standards for Windows 2003 Servers* to clearly define system administrator responsibilities for maintaining and regularly updating Active Directory objects.

Security Standards Compliance

Domain controllers[3] running on Windows operating systems did not comply with requirements documented in the Postal Service Windows security standards. This occurred because management did not perform a comprehensive review of server configurations against the Windows security standards and properly maintain the security standards document. By ensuring that server configuration settings comply with Postal Service policy,[4] management can strengthen security over information resources to protect against accidental or intentional unauthorized use, modification, disclosure, or destruction. See Appendix B for our detailed analysis of this topic.

We recommend the manager, Corporate Information Security, in coordination with the manager, Information Technology Engineering and Architecture, perform:

2. A review of the *Security Standards for Windows 2003* and update the standards as appropriate.

3. A comprehensive review of the domain controller configurations to ensure compliance with applicable Windows security standards.

Management's Comments

Management agreed with our recommendations. In response to recommendation 1, management accepts the recommendation to review the *Security Standards for Windows 2003* servers, but believes the roles and responsibilities assignment does not belong in the *Security Standards for Windows 2003 Server's* documents. They believe the roles and responsibilities belong in operational roles and responsibility guidelines because the system administrator's responsibilities are consistent across the Windows platform. The targeted completion date is April 30, 2010.
To address recommendation 2, management will review the current hardening *Security Standards for Windows 2003 Servers* to determine if any changes are required. Management is currently testing *Security Standards for Windows 2008* and servers under *Security Standards for Windows 2003* will be migrated to that environment.

[3] A server that responds to security authentication requests (including logging in and checking permissions) within the Windows server domain. A domain controller physically stores Active Directory information. Large domains require more than one domain controller, where each holds a copy of Active Directory. Active Directory synchronizes any computer changes between all domain controllers, called "multi-master replication".
[4] *Security Standards for Windows 2003 Servers*, Section 3.10, Operating System Security Settings.

Subsequent discussions with management revealed that the target date for completion of the *Security Standards for Windows 2008* is September 30, 2010.

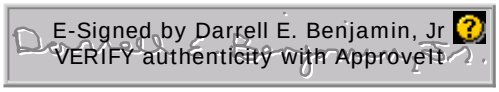
In response to recommendation 3, management will review the domain controller configurations to ensure compliance with applicable Windows security standards for domain controller. The targeted completion date is April 30, 2010. See Appendix C for management's comments in their entirety.

Evaluation of Management's Comments

The U.S. Postal Service, Office of Inspector General (OIG) considers management's comments responsive to the recommendations, and their corrective actions should resolve the issues identified in the report.

The OIG considers recommendation 3 significant, and therefore requires OIG concurrence before closure. Consequently, the OIG requests written confirmation when corrective actions are completed. This recommendation should not be closed in the Postal Service's follow-up tracking system until the OIG provides written confirmation that the recommendation can be closed.

We appreciate the cooperation and courtesies provided by your staff. If you have any questions or need additional information, please contact Frances E. Cain, director, Information Technology, or me at (703) 248-2100.



Darrell E. Benjamin, Jr.
Deputy Assistant Inspector General
for Revenue and Systems

Attachments

cc: Deborah J. Judy
Gregory "Dean" Larrabee
Cliff M. Biram
Sally K. Haring

APPENDIX A: ADDITIONAL INFORMATION

BACKGROUND

Logical access controls include the use of computer hardware and software to prevent or detect unauthorized access. For example, a system or information resource may require users to authenticate with a logon identification, user name, password, or other identifier that conforms to the concepts of least privilege and need-to-know. Inadequate access controls diminish the reliability of computerized data and increase the risk of destruction or inappropriate disclosure of data.

The [redacted] is the enterprise directory for the Postal Service. It is the authoritative source for all centrally supported and managed Windows-based systems. The Postal Services bases access to all infrastructure platforms, remote access methods, and national applications on user and machine credentials in the [redacted] Active Directory. Microsoft Windows Active Directory[5] enables single-point administration to organize, manage, authenticate, and control information within the Windows environment. Information Technology Engineering and Architecture staff located at the [redacted] supports the Active Directory.

OBJECTIVE, SCOPE, AND METHODOLOGY

The objective of this audit was to determine whether the Postal Service established adequate logical controls to limit or detect inappropriate access to its Windows operating environment.

[redacted].

To accomplish the objective, we reviewed Postal Service documentation and available policies and procedures, interviewed key officials, and examined other material deemed necessary to accomplish our objective[redacted]

[5] The latest version of Microsoft Windows Server 2008 R2 renamed Active Directory to Active Directory Domain Services.

[6] [redacted].

We conducted this performance audit from June 2009 through March 2010 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 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, 2010, and included their comments where appropriate. We used manual and automated techniques to analyze the data obtained from the domain controllers. Based on the results of these tests and assessments, we concluded the data were sufficient and reliable to use in meeting the objective.

PRIOR AUDIT COVERAGE

Report Title	Report Number	Final Report Date	Report Results
Access Controls [redacted]	IS-AR-08-015	8/15/2008	We reviewed the following two applications operating in a Windows environment: [redacted]. Our review verified that management implemented proper access controls, providing reasonable assurance that data files and application programs are protected against unauthorized modification, disclosure, loss or impairment. We found no issues associated with the applications reviewed.
System Software Controls [redacted]	IS-AR-08-011	6/3/2008	We reviewed three application servers covering [redacted] in the Windows environment. Our review verified that management implemented proper access controls, procedures for monitoring software infrastructure, and controls for change and configuration management. We found no issues associated with the specific applications reviewed.

Report Title	Report Number	Final Report Date	Report Results
Information Systems Access Controls at Selected Information Technology Facilities for Fiscal Year 2007	IS-AR-08-002	11/6/2007	We evaluated Active Directory security settings and found Windows default password settings did not comply with Postal Service Policy.[7] Management agreed and implemented the recommendation to change the default password settings according to policy requirements.
System Software Controls [redacted]	IS-AR-07-013	8/3/2007	We reviewed Windows systems controls over auditing, domain controllers, and global settings. We verified that management appropriately configured the Windows operating system at the domain level and that the domain global settings record all accesses to system files. We verified that management used system utilities such as Active Directory, BMC Patrol, Microsoft Operations Manager, Systems Management Server 2003, and Symantec Anti-Virus[8] to enhance security. We did not make any recommendations in this report.
Information System Access Controls [redacted]	IS-AR-06-018	9/27/2006	We found Windows access controls were adequate to protect computer and information resources at the data centers against unauthorized modification, loss, and disclosure. We found no issues associated with the specific applications.

[7] Handbook AS-805

[8] BMC Patrol monitors the performance and availability of servers, applications, and storage and network devices. Microsoft Operations Manager is a performance and event-monitoring product from Microsoft targeting Windows systems. Systems Management Server 2003 validates software loaded on workstations and servers. Symantec Anti-Virus detects and prevents virus attacks.

APPENDIX B: DETAILED ANALYSIS

Active Directory Management

System administrators were not updating the Active Directory OUs, groups, and accounts [redacted] For example, administrators did not:

- Group distribution lists for [redacted] with the distribution lists for the [redacted]
- Remove an [redacted] backup account assigned to a terminated employee.
- Remove unused Active Directory objects such as test accounts and a printer OU.
- Delete unused OUs, [redacted].
- Move an Active Directory group from an incorrect OU to the correct OU.

This occurred because administrators do not have clearly defined responsibilities for maintaining and updating Active Directory objects regularly. Postal Service policies require the periodic review and update of accounts to restrict access according to the least-privilege and need-to-know principles.[9]

By properly maintaining Active Directory objects, management can reduce the risk of unauthorized access to Postal Service information resources, access authority that exceeds job responsibilities, and operational disruptions.

Prompted by our review, management began corrective action to update and remove obsolete objects. Additionally, an initiative within eAccess[10] has a new automated feature that will facilitate the reconciliation on certain types of accounts to enhance security over Active Directory.

Security Standards Compliance

Domain controllers running on the Windows operating systems did not comply with the requirements documented in the latest Postal Service Windows security standards. These standards contain approximately 150 required security settings. On the three servers reviewed, we found 32 of the 150 settings – [redacted] – that did not comply with the Windows security standards. This occurred because management was not performing a comprehensive review of server configurations against the Windows security standards and maintaining the security standards document. Management periodically runs a script to review server configurations. The script retrieves the results of approximately 80 security settings that address Sarbanes-

[9] *Security Standards for Windows 2003 Servers,* Section 1.2 and Handbook AS-805, Section 9-3.2.5.
[10] eAccess provides automated access management capabilities to Postal Service information resources, including [redacted] accounts, applications, and databases.

Oxley requirements. Postal Service policy[11] requires management to adhere to the security standards and review operating system configurations periodically. Management can strengthen security over information resources to protect against accidental or intentional unauthorized use, modification, disclosure, or destruction by ensuring server configuration settings comply with Postal Service policy.[12]

[11] Handbook AS-805, Section 8-5.4.2, Harden Information Resources; Section 10-2.3.1, Hardening Servers.
[12] *Security Standards for Windows 2003 Servers*, Section 3.10, Operating System Security Settings.

APPENDIX C: MANAGEMENT'S COMMENTS

ROSS PHILO
EXECUTIVE VICE PRESIDENT
CHIEF INFORMATION OFFICER

UNITED STATES POSTAL SERVICE

March 12, 2010

Lucine M. Willis
Director, Audit Operations
Office of Inspector General
1735 N. Lynn Street, Room 11044
Arlington, VA 22209-2020

SUBJECT: Transmittal of Draft Audit Report – Windows Access Controls at the Information Technology and Accounting Service Centers – IS General Controls FY 2009 (Report Number umber IS-AR-10-XXX) Project Number 09RD001IS005

Thank you for the opportunity to review and comment on the subject draft audit report. We are in agreement with recommendations 1, 2, and 3 of the report; the response is attached.

[redacted]

If you have any questions or comments regarding this response please contact Gerri Wallace, Corporate Information Security at (202) 268-6821.

Ross Philo

Attachment

cc: Debbie J. Judy
Gregory "Dean" Larrabee
Cliff M. Biram
Sally K. Haring

475 L'ENFANT PLAZA SW
WASHINGTON, DC 20260-1500
202-268-6900
FAX: 202-268-4492
ROSS.PHILO@USPS.GOV
WWW.USPS.COM

We recommend the manager, Corporate Information Security Office, work with the manager, Information Technology Engineering and Architecture, to:

1. Revise the *Security Standards for Windows 2003 Servers* to clearly define system administrator responsibilities for maintaining and regularly updating Active Directory objects.

   Management accepts the recommendation to review the *Security Standards for Windows 2003 Servers*; however, we believe that the roles and responsibilities assignment does not belong in the *Security Standards for Windows 2003 Server's* documents. The role and responsibilities belongs in an "operational roles and responsibility guideline" because the system administrator's responsibilities are consistent across the Windows platform.

   Anticipated completion date: April 30, 2010

2. A review of the Security Standards for Windows 2003 and update the standards as appropriate.

   Management agrees with the recommendation and will review the current hardening *Security Standards for Windows 2003 Servers* to determine if any changes are required. However, we are currently testing *Security Standards for Windows 2008 Servers* and servers under *Security Standards for Windows 2003* will be migrated to that environment.

   Anticipated completion date: Requesting closure upon receipt.

3. A comprehensive review of the domain controller configurations to ensure compliance with applicable Windows security standards.

   Management agrees with the recommendation and will review the domain control configuration to ensure compliance with the applicable Windows security standards for domain controller.

   Anticipated completion date: April 30, 2010