February 20, 2009

GEORGE W. WRIGHT
VICE PRESIDENT, INFORMATION TECHNOLOGY OPERATIONS

SUBJECT: Audit Report – Access Controls in the Enterprise Data Warehouse (Report Number IS-AR-09-004)

This report presents the results of our audit of access controls in the Enterprise Data Warehouse (EDW) (Project Number 08RG027IS000). The report is the result of a self-initiated audit, which addresses operational risk. See Appendix A for additional information about this audit.

Conclusion

Overall, we believe the U.S. Postal Service has been diligent in its efforts to secure sensitive information stored in EDW from inappropriate access. However, management needs to strengthen access controls governing contractors who are nonstandard users of the system, update the Business Impact Assessment (BIA), recertify EDW, and simplify how EDW managers assign and maintain access rights.

Contractor Access to Enterprise Data Warehouse

Access controls are not adequate for EDW nonstandard users[1] who are contractors. Our analysis showed that for 90 out of 107 contractors (84 percent), their justifications for continued access to EDW listed on Postal Service (PS) Forms 1357, Request for Computer Access, referenced contracts that had expired. Further, we found that 72 of the 90 contractors (80 percent) with expired contracts listed had logged into EDW after their contract expiration date. We contacted several of these contractors and determined they were working on other Postal Service contracts. However, their supporting documentation did not reflect that information, and we could not determine whether their work on these contracts justified their continuing access to EDW.

This occurred because the Postal Service does not track contractors' access to the EDW application or their contract expiration date. In addition, the Postal Service

[1] Nonstandard users of EDW have access to the actual data in the system, unlike standard users, who can view only the reports generated from EDW but cannot access the actual data.

elected not to use eAccess[2] as a tracking mechanism. EDW managers said they had not used eAccess for nonstandard users in the past because eAccess did not provide the additional levels of approval they thought were necessary. Requests for nonstandard access to EDW through eAccess should require additional levels of approval, much like the current process for approving PS Forms 1357. Managers indicated that if eAccess provided the option of selecting nonstandard access, rather than standard access only, they would prefer to use eAccess. Postal Service policy[3] requires managers to revoke access to information when an employee no longer requires it. Managers' not revoking a contractor's access when a contract expires could result in unauthorized individuals having access to sensitive EDW information.

We recommend the Vice President, Information Technology Operations, direct the Manager, Business Data Management, to:

1. Set expiration dates for contractors' access on or before the expiration date of the contracts they use to justify their access to the Enterprise Data Warehouse.

2. Use eAccess to request and approve access for nonstandard users of the Enterprise Data Warehouse, and update eAccess to enable the requestor to select standard or nonstandard access.

Enterprise Data Warehouse Recertification

Information in the EDW BIA is not currently up to date. EDW has grown significantly since its Information Security Assurance (ISA) certification in June 2004. EDW is designed to store data from multiple Postal Service applications. As such, it is critical that management complete the ISA and BIA process for each business area component that feeds into EDW and provide the information to EDW managers. EDW managers should also consider the business application ISA information in the updated BIA for EDW. Postal Service policy[4] states that management must reinitiate the ISA a minimum of every 5 years following its initial application, or when a significant change occurs in the operating environment, business requirements, or application. In addition, the Enterprise Information Repository lists EDW as needing recertification every 3 years, which means recertification was due June 24, 2007.

Management was not aware of the requirement to update the BIA for EDW. Therefore, EDW has not been recertified. In addition, EDW managers stated that the business

[2] The eAccess system has become an integral part of the day-to-day operations of the Postal Service. The system not only monitors who obtains access to various Postal Service resources, but also automates the creation and maintenance of user accounts. Its functionality provides efficiencies that allow for the elimination of PS Form 1357, and the associated manual effort necessary to approve and create user accounts.
[3] Handbook AS-805, *Information Security*, dated March 2002 (updated with *Postal Bulletin* revisions through November 23, 2006), Chapter 9, Information Security, Section 4.2.7: Revoking Access.
[4] Handbook AS-805-A, *Application Information Security Assurance (ISA) Process*, dated July 2003 (updated with *Postal Bulletin* revisions through September 29, 2005), Chapter 6, Re-Initiating the ISA, Section 6-2, When Re-ISA is Required.

areas that have applications located within EDW have not provided a current BIA for their applications. Our audit identified 45 sensitive applications that feed into EDW. As of January 2, 2009, nine[5] of these systems had not completed a BIA. Consequently, EDW managers have reason to question the reliability of the information available to them about which data elements are sensitive. As a result, unauthorized users may have access to sensitive data, which could also create a risk to the integrity of the Postal Service brand.

We recommend the Vice President, Information Technology Operations, direct the Manager, Business Data Management, to:

3. Update the Business Impact Assessment for the Enterprise Data Warehouse and recertify the system as required by Postal Service Handbook AS-805-A, *Application Information Security Assurance (ISA) Process*.

We recommend the Vice President, Information Technology Operations, direct the Manager, Corporate Information Technology Portfolios, to:

4. Ensure all business areas that feed data into the Enterprise Data Warehouse provide a current Business Impact Assessment for their applications to the Enterprise Data Warehouse Program Manager, Information Technology; the Business Impact Assessment should verify which data elements are sensitive and need additional security measures.

EDW Access Rights

The current process for assigning and managing access rights within EDW is very complicated and too time-consuming to manage effectively. This occurred because management assigns rights to individuals, roles, and nested roles as a matter of practice. Our request for information on the detailed rights for 130 users returned over 300,000 lines of data. Management would need to analyze each line of data to determine the detailed rights for these individuals, and whether the rights granted are appropriate.

Best practices[6] encourage access to computer applications and systems to be role based, which means that management grants permissions to roles. Management makes users members of roles, so the users acquire the permissions granted to the roles. Because managers do not assign user permissions exclusively to roles, they have little knowledge about users' rights in EDW. Managers could also misinterpret

[5] Customer Advocate Management System, Vehicle Management and Accounting System, Supply Chain Management, Accounting Data Mart, Complement Management and Selection, Safety and Health, Electronic Marketing Reporting System, Unique Customer Identification, and Employee Receivables.

[6] Planning Report 02-1, *The Economic Impact of Role-Based Access Control*, prepared by the Rochester Institute of Technology for National Institute of Standards and Technology, Program Office Strategic Planning and Economic Analysis Group, dated March 2002, Chapter 2, The Evolution of Role-Based Access Controls, Section 2.1.1, Users, Roles, and Permissions.

access rights for an individual and provide access to sensitive information to users who do not need the information.

We recommend the Vice President, Information Technology Operations, direct the Manager, Business Data Management, to:

5. Assign access rights to roles instead of to individual and nested roles.

Management's Comments

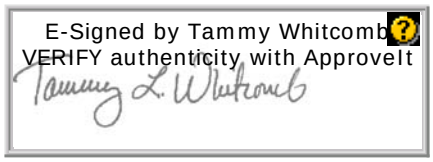
Management agreed with all of the recommendations and stated that Business Data Management will reevaluate the process for all contractors requesting access for EDW to ensure they do not have access rights after the contract period has expired. The scheduled completion date is July 30, 2009. Further, management will update and use eAccess as the mechanism for approving access for non-standard users by April 17, 2009. Business Data Management will also update the BIA and recertify the EDW as required by August 28, 2009. In addition, Corporate Information Technology will ensure that current BIAs are in place for business areas that feed data into the EDW, and will also verify which data elements are sensitive and require additional security measures by May 31, 2009. Finally, management agreed they need to assign access rights to roles instead of individuals. Management will reevaluate access rights and analyze nested roles to determine if they can improve the current process by July 30, 2009. See Appendix B 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 corrective actions should resolve the issues identified in the report.

The OIG considers recommendations 1, 2, 3, and 4 significant, and therefore requires OIG concurrence before closure. Consequently, the OIG requests written confirmation when corrective actions are completed. These recommendations should not be closed in the Postal Service's follow-up tracking system until the OIG provides written confirmation that the recommendations can be closed.

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



Tammy L. Whitcomb
Deputy Assistant Inspector General
for Revenue and Systems

Attachments

cc: Ross Philo
Harold E. Stark
John T. Edgar
Greg G. Wallace
Jerry McClure
Katherine S. Banks

APPENDIX A: ADDITIONAL INFORMATION

BACKGROUND

A data warehouse is a collection of data from many sources, stored in a single place for reporting and analysis. A data mart is a repository of data gathered from operational data and other sources that is designed to serve a community of knowledge workers. In general, a data warehouse tends to be a strategic, but somewhat unfinished, concept; a data mart tends to be tactical and aimed at meeting an immediate need.

The Postal Service has traditionally stored data in older systems (called legacy systems) that are by nature stove-piped, or self-contained; therefore, these systems are inaccessible for use with other data or by other business organizations. Because of overlapping needs, various systems often contain the same information, which may or may not produce the same reporting results from system to system. The EDW is a collection of data from many sources that is stored in a single place for reporting and analysis. It provides a single repository for managing all of the Postal Service's data assets for a wide variety of users. The data can be divided in various ways within and across functions for deeper analysis, which can lead to additional revenue, reduced costs, and improved business practices. Several Postal Service organizations have data in EDW, including, but not limited to, Retail, Supply Chain Management, Finance, Network Operations, and Facilities. The primary reporting tool is a web-based tool from MicroStrategy, Inc., which offers greater functionality than is possible with Postal Service systems and reporting tools.

OBJECTIVE, SCOPE, AND METHODOLOGY

The objective of this audit was to determine if access controls were adequate to prevent inappropriate access to sensitive information in the EDW. To accomplish our objective, we reviewed documentation, policies, and procedures and interviewed key officials within the Business Data Management group in Raleigh, NC; Information Technology in Eagan, MN; and Corporate Information Security in Washington, DC. In addition, we reviewed the Enterprise Information Repository to determine which applications feeding into EDW were sensitive. We also obtained a list of current nonstandard users of EDW who are contractors. We obtained and reviewed[7] contractors' PS Forms 1357 to determine, based on the contract expiration date, whether the justification for access was valid, and to identify contractors' rights and access they had within EDW. We compared contractors' last login dates in EDW with contract expiration dates to determine whether contractors were still accessing information within EDW after their contract expired. In addition, we contacted a selection of nonstandard users of EDW whose employee status was missing from our data to determine whether they were Postal Service employees or contractors.

[7] We reviewed 107 of a total of 112 (96 percent) contractors who had nonstandard access to EDW. We were unable to locate five of these files.

We worked with Postal Service officials to develop a switch user test, which meant finding an existing script that a nonstandard user uses and editing it so a different user could accomplish the same task. In addition, we interviewed Postal Service officials who create and review scripting logs of the EDW, and we reviewed policy for scripting logs. We also ran a test to query the EDW logs to verify that the required logs were being created. To verify the existence of two required logs deemed too sensitive to create views, we observed nonstandard users with administrative rights gaining direct access to these logs.

We conducted this performance audit from June 2008 through February 2009 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 officials on January 14, 2009, and included their comments where appropriate. We determined that the computer-generated data used to support our findings was sufficiently reliable for the purposes of this audit. We validated this information by conducting interviews and reviewing hardcopy documentation (PS Forms 1357) that supported data extracted from EDW.

PRIOR AUDIT COVERAGE

In our report titled, *Update Processes for Active Directory and CA-ACF2 (*Report Number IS-AR-08-009, dated March 14, 2008), we recommended making improvements to the approval process and tracking detailed employees in eAccess to help strengthen security controls. Management has implemented the planned eAccess enhancement that will ensure access reviews take place and has updated system documentation for eAccess. However, management has not yet determined how to integrate managers' roles so the Human Capital Enterprise System can pass accurate and timely employment change data to eAccess or the system for tracking employees who are on detail.

APPENDIX B: MANAGEMENT'S COMMENTS

GEORGE W. WRIGHT
VICE PRESIDENT
INFORMATION TECHNOLOGY OPERATIONS

UNITED STATES POSTAL SERVICE

February 12, 2009

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

SUBJECT: Draft Audit Report – Review of Access Controls in the Enterprise Data Warehouse (Report Number IS-AR-09-00X-Project Number 08RG027IS000)

Thank you for the opportunity to review and comment on the subject draft audit report. We are in agreement with recommendations 1, 2, 3, 4 and 5 of the report and the response is attached.

The subject report and this response contain information related to potential security vulnerabilities that, if released, could possibly be exploited and cause substantial harm to the U.S. Postal Service. The Manager, Corporate Information Security will work with you to determine what portions of this report should be considered as classified and restricted and exempt from disclosure under the Freedom of Information Act.

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

George W. Wright

Attachment

cc: Ross Philo
Harold E. Stark
John T. Edgar
Greg G. Wallace
Jerry McClure
Katherine S. Banks
audittracking@uspsoig.gov

475 L'ENFANT PLAZA SW
WASHINGTON, DC 20260-1500
202-268-2764
FAX: 202-268-4492
GEORGE.W.WRIGHT@USPS.GOV
WWW.USPS.COM

Review of Access Controls in the Enterprise Data Warehouse (Report Number IS-AR-09-00X)
(Project Number 08RG027IS000 – Page 1 of 2)

We recommend the Vice President, Information Technology Operations; direct the Manager, Business Data Management, to:

1. Set expiration dates for contractors' access on or before the expiration date of the contract they use to justify their access to the Enterprise Data Warehouse (EDW).

   Management Response
   Management agrees. Manager, Business Data Management will reevaluate the process for all contractors requesting access for EDW to ensure contractors do not have access to EDW after the contract has expired.

   Scheduled Completion Date: July 30, 2009

2. Use eAccess as the mechanism for requesting and approving access for non-standard users of the Enterprise Data Warehouse and update eAccess to enable the requestor to select standard or non-standard access.

   Management Response
   Management agrees. Manager, Business Data Management will use eAccess as the mechanism for the approval process and update eAccess to enable the requestors to select standard or non-standard access.

   Scheduled Completion Date: April 17, 2009

3. Update the Business Impact Assessment for the Enterprise Data Warehouse and recertify the system as required by Postal Service Handbook AS-805 A, *Application Information Security Assurance (ISA)* Process.

   Management Response
   Management agrees. Manager, Business Data Management will update the ISA/IIA for EDW.

   Scheduled Completion Date: August 28, 2009

Review of Access Controls in the Enterprise Data Warehouse (Report Number IS-AR-09-00X)
(Project Number 08RG027IS000 – Page 2 of 2)

We recommend the Vice President, Information Technology Operations; direct the Manager, Corporate Information Technology Portfolios, to:

4. Ensure all business areas that feed data into the Enterprise Data Warehouse provide a current Business Impact Assessment for their application to the Enterprise Data Warehouse Program Manager, Information Technology, that also verifies which data elements are sensitive and need additional security measures.

Management Response

Management agrees. Manager, Corporate Information Technology Portfolios will ensure that current Business Impact Assessments (BIA) are provided for all sensitive applications interfacing with EDW including listing all sensitive data elements that are passed to the EDW and any required security measures, where applicable. IT Management will work with the OIG to validate the list of the 45 applications as there appears to be incorrect and duplicative information.

Scheduled Completion Date: May 31, 2009

We recommend the Vice President, Information Technology Operations; direct the Manager, Business Data Management, to:

5. Assign access rights to roles instead of individual and nested roles.

Management Response

Management agrees. Manager, Business Data Management will reevaluate the access rights to analyze nested role to determine if the process can be improved.

Scheduled Completion Date: July 30, 2009