Susan Montee, CPA

Missouri State Auditor

TRANSPORTATION

Carrier Express System Data Security

January 2009

Report No. 2009-04

auditor.mo.gov

Susan Montee, CPA
Missouri State Auditor

YELLOW SHEET

Important Security Controls Are in Place, but Work Remains to Ensure the Confidentiality and Integrity of System Data and Information

This audit reviewed the Missouri Department of Transportation (MoDOT) Carrier Express System. Auditors found MoDOT management established many of the security controls necessary to protect the confidentiality, integrity and availability of data and information in the Carrier Express System. However, MoDOT management needs to establish additional controls to better ensure the confidentiality and integrity of data.

System has been operating as designed	The Carrier Express System had been operating as MoDOT management designed. The critical functions of collecting, processing, storing and reporting motor carrier data have been reliably performed. Except as noted in the following two sections, data confidentiality and integrity have been ensured through controls over the input, processing, storage and output of system data. (See page 5)
Review of user account access rights needed	MoDOT Motor Carrier Services management had not ensured user access rights remained commensurate with job responsibilities by performing regular reviews of user accounts and related access rights or privileges. Requiring a review of all user accounts ensures the right type and level of access has been provided. Without reviewing user access rights, management cannot ensure access rights are appropriate for the user's responsibilities resulting in an increased risk of unauthorized access, modification, use or disclosure of data. (See page 5)
Insurance agents' access should be restricted	Insurance agents had access to change insurance policy information in the Carrier Express System for all motor carriers, including carriers not insured with the agent. Accepted standards require information systems to enforce the most restrictive set of rights, privileges or accesses needed by users. Without a control to restrict access, insurance agents had the ability to make unauthorized changes and motor carriers could have been granted the authority to operate without having the required insurance. (See page 6)

Contents

State Auditor's Letter 2

Important Security Controls Are in Place, but Work Remains to Ensure the Confidentiality and Integrity of System Data and Information 3

Background 3
Scope and Methodology 4
System Was Operating As Designed 5
Review Of User Account Access Rights Needed 5
Insurance Agents' Access Should Be Restricted 6
Conclusions 7
Recommendations 7
Agency Comments 7

Abbreviations

ISD	Missouri Department of Transportation Information Systems Division
MCS	Motor Carrier Services
MoDOT	Missouri Department of Transportation
SAO	State Auditor's Office

SUSAN MONTEE, CPA
Missouri State Auditor

Honorable Matt Blunt, Governor
and
Missouri Highways and Transportation Commission
and
Pete K. Rahn, Director
Department of Transportation
Jefferson City, MO

The Missouri Department of Transportation (MoDOT) Motor Carrier Services Division is responsible for the oversight of commercial motor carriers in Missouri, including licensing, registration, safety and compliance. The MoDOT Carrier Express System was audited based on the results of a risk assessment performed during our recent audit at the MoDOT titled *Information Systems Security Controls (Report No. 2008-49)*. Our audit objective included determining whether MoDOT management established adequate security controls to ensure the confidentiality, integrity and availability of data and information in the MoDOT Carrier Express System.

We concluded MoDOT management established many of the security controls necessary to protect the confidentiality, integrity and availability of data and information in the Carrier Express System. However, MoDOT management needs to establish additional controls to better ensure the confidentiality and integrity of data. Management had not periodically reviewed user accounts to ensure access remained appropriate and had not established controls to restrict the access of insurance agents.

We conducted our audit in accordance with the standards applicable to performance audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States. Those standards require that we plan and perform our audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides such a basis. This report was prepared under the direction of John Luetkemeyer. Key contributors to this report included Jeff Thelen, Lori Melton, and Richard Mosha.

Susan Montee, CPA
State Auditor

Important Security Controls Are in Place, but Work Remains to Ensure the Confidentiality and Integrity of System Data and Information

Missouri Department of Transportation (MoDOT) management established the Carrier Express System, an online information system, to collect, process, store and output motor carrier data and information. Management established many of the security controls necessary to protect the confidentiality, integrity and availability of data and information in the system. However, additional controls need to be established to better ensure the confidentiality and integrity of data. Management had not (1) reviewed user accounts to ensure access remained appropriate and (2) restricted access of insurance agents to motor carrier policy information to only those carriers covered by each insurance agency. These access control weaknesses reduce the MoDOT's ability to ensure the confidentiality and integrity of data and information in the system.

Background

The MoDOT Motor Carrier Services (MCS) Division provides motor carriers[1] with the information, credentials and permits needed to conduct business in Missouri, according to the MCS website.[2] MCS also enforces commercial vehicle safety and economic regulations, including insurance requirements.

The Carrier Express System maintains confidential data including carriers' Social Security and Federal Identification Numbers. MoDOT management paid a contractor a total of approximately $15 million during fiscal years 2005 through 2008, for the creation, implementation and maintenance of the system. The system was accepted by MoDOT management in February 2007, according to an Information Systems Division (ISD) official. According to MCS staff, the system processed transactions totaling approximately $164 million in fiscal year 2008.

The Carrier Express System was designed to meet the needs of various users:

- Motor carriers access the system to update contact information; apply and pay for licensing, registration and permits; provide required information such as miles driven and fuel tax paid; and print necessary permits.
- MCS employees access the system to perform job duties to support motor carriers and enforce regulations.

[1] According to Missouri Revised Statutes, a motor carrier is any person engaged in the transportation of property or passengers, or both, for compensation or hire, over the public roads of this state by motor vehicle (Section 390.020, RSMo).

[2] "Who We Are, What We Do, Key Programs," MoDOT Motor Carrier Services, <http://www.modot.mo.gov/mcs/documents/WhoWeAre2006.pdf>, accessed October 30, 2008.

- Insurance agents access the system to update insurance policy information for motor carrier customers.
- Department of Natural Resources employees access the system to review and approve applications to haul hazardous waste and waste tires.
- ISD employees support the system.

According to accepted standards, security controls are the management, operational, and technical safeguards or countermeasures prescribed for an information system[3] to protect the confidentiality, integrity, and availability of the system and its information. Confidentiality refers to preserving authorized restrictions on information access and disclosure, including the means for protecting personal privacy and proprietary information. Integrity relates to guarding against improper information modification or destruction and availability ensures timely and reliable access to and use of information.

Scope and Methodology

To determine whether MoDOT management had established adequate security controls to ensure the confidentiality, integrity and availability of data and information in the MoDOT Carrier Express System, we conducted interviews with appropriate MoDOT officials and staff; requested and reviewed available policies, procedures and other information; obtained and reviewed financial reports prepared by the system; obtained and reviewed the system's disaster recovery plan; and performed testing.

We obtained data files from the ISD containing the various user accounts having access to the system as of August and September 2008. These files contained over 35,000 user accounts, of which 34,000 had been assigned to motor carrier users. To verify completeness of the data, we ensured all MCS employees had been accounted for by comparing the MCS organization chart to the listing of user accounts.

We obtained the employment records for MoDOT employees for fiscal years 2001 through 2008 from the statewide accounting system for human resources. We did not perform specific procedures to ensure reliability because the risk of unreliable results was considered insignificant. We matched this data to the user accounts to determine if any terminated employees had active user accounts. We provided an ISD official with a list of all user accounts we identified that were associated with terminated employees.

[3] Accepted standards define an information system as a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

We based our work on accepted state, federal, national and international standards and best practices related to information technology security controls from the following sources:

- Missouri Adaptive Enterprise Architecture[4]
- National Institute of Standards and Technology (NIST)
- U.S. Government Accountability Office (GAO)
- IT Governance Institute Control Objectives for Information and related Technology (COBIT)

We limited our review to the specific matters described above and based it on selective tests and procedures considered appropriate in the circumstances. Had we performed additional procedures, other information might have come to our attention that would have been included in the report.

System Was Operating As Designed

We found the Carrier Express System had been operating as MoDOT management designed. The critical functions of collecting, processing, storing and reporting motor carrier data had been reliably performed. Except as noted in the following two sections, data confidentiality and integrity had been ensured through controls over the input, processing, storage and output of system data. Audit trails were available for review, if needed, to trace transactions through the system. In addition to internal reviews of financial transactions, individuals from the MoDOT Controller's Office reconciled revenues received to bank information and reviewed payments processed by the system. ISD management had documented a disaster recovery plan to ensure system availability.

Review Of User Account Access Rights Needed

MCS management had not ensured user access rights remained commensurate with job responsibilities.[5] According to accepted standards, there should be regular reviews of all user accounts and related access rights or privileges. Requiring a review of all user accounts ensures the right type and level of access has been provided. Otherwise, user accounts and accesses can be granted to or maintained for users who should not have

[4] The Enterprise Architecture includes standards, policies and guidelines established by the Office of Administration, Information Technology Services Division. The Enterprise Architecture is made up of several information technology domains, including domains dedicated to security and information. The domains are not fully developed, but define the principles which are needed to help ensure the appropriate level of protection for the state's information and technology assets.

[5] This situation was addressed department-wide during our recent audit at MoDOT, titled *Information Systems Security Controls*, SAO, August 2008 (Report No. 2008-49).

access, according to accepted standards. During our review of system user accounts, we identified:

- User accounts assigned to 12 motor carriers with access to financial groups that allow users to process cash or check transactions, a function that motor carriers should be restricted from performing, according to an ISD official.
- User accounts assigned to 6 ISD employees with access to financial transactions. This access was removed for 3 accounts after we discussed technology employees having access to financial transactions with ISD officials. According to the officials, the 3 remaining ISD accounts need access for system troubleshooting purposes. According to accepted standards, technology personnel should not have end user responsibilities. However, the MoDOT Controller's Office staff reconciles the revenues and bank accounts daily, which reduces the risk of financial transactions being processed without the accompanying revenue flow.
- A shared user account. According to ISD officials, this account had been shared by 4 or 5 people. This account had administrative access and access to override transactions.
- User accounts granted access rights not needed to perform job duties. Of the 115 user accounts assigned to security groups or groups with access to override transactions, 8 (7 percent) should not have been assigned to the group reviewed, according to MoDOT officials.
- A user account for a terminated employee. This account had access to override transactions.
- A MCS employee with a second user account.
- Accounts for 22 users not assigned to any security group. These accounts could not access any system functions and were unnecessary, according to an ISD official.

Without periodically reviewing user access rights, management cannot ensure access rights are appropriate for each user's responsibilities resulting in an increased risk of unauthorized access, modification, use or disclosure of data.

Insurance Agents' Access Should Be Restricted

Insurance agents had access to change insurance policy information for all motor carriers, including carriers not insured with the agent. Accepted standards require information systems to enforce the most restrictive set of rights, privileges or accesses needed by users.

Motor carriers are required to have insurance to be granted authority to operate in Missouri and the insurance must be verified by the issuing insurance agent, according to MCS staff. Insurance agents are granted access to the Carrier Express System to provide this verification. However,

this access did not restrict agents to only information for carriers insured with the agent. Instead, each insurance agent had access to update insurance policy information for all motor carriers in the system. A mechanism or control had not been established to ensure insurance agents could only change the insurance information of each agent's customers, according to MCS staff. Without a control to restrict access, insurance agents had the ability to make unauthorized changes and motor carriers could have been granted the authority to operate without the required insurance.

Conclusions

The Carrier Express System had been operating as MoDOT management designed, reliably performing the critical functions of collecting, processing, storing and reporting motor carrier data and information. MoDOT management had done an effective job establishing many of the security controls needed to protect the confidentiality, integrity and availability of data. However, to better protect the confidentiality and integrity of data and information in the system, MoDOT management needs to establish controls for the periodic review of user accounts and to restrict the access of insurance agents.

Recommendations

We recommend the Director of the Department of Transportation:

1.1 Periodically review user accounts to ensure access remains appropriate. Access should be modified or removed as necessary.

1.2 Restrict the access of insurance agents to only the policy information for those motor carriers insured with the agent. If a system control cannot be established to restrict access, MoDOT officials should implement a process to review and monitor changes to insurance data.

Agency Comments

1.1 MoDOT concurs with the recommendation to periodically review user accounts to ensure access remains appropriate. MoDOT Motor Carrier Services user accounts have been manually reviewed to ensure current access is appropriate. In addition, an ongoing review of MCS user accounts will be conducted annually.

1.2 MoDOT concurs with the recommendation to restrict the access of insurance agents to only the policy information for those motor carriers insured with the agent. New functionality was implemented on December 8, 2008, that prohibits insurance agents from accessing any motor carrier information other than the ones they represent.