PERFORMANCE AUDIT

DEPARTMENT OF REVENUE
INFORMATION RESOURCE SECURITY MANAGEMENT

From The Office Of State Auditor
Claire McCaskill

Tighter security controls need to be in place to reduce the existing risk of unauthorized access to department resources.

Report No. 2003-16
February 20, 2003
www.auditor.state.mo.us

DEPARTMENT OF REVENUE
INFORMATION RESOURCE SECURITY MANAGEMENT

TABLE OF CONTENTS

Page

STATE AUDITOR'S REPORT 1

RESULTS AND RECOMMENDATIONS 2

1. Controls Over System Access are Weak or Missing 2

   Conclusion 9

   Recommendations 10

2. The Department Lacks a Computer Security Management Program 13

   Conclusion 16

   Recommendations 16

3. Physical Security Controls are Not Adequate 18

   Conclusion 18

   Recommendations 18

APPENDIXES

I. OBJECTIVE, SCOPE AND METHODOLOGY 20

II. DEFINITION OF TERMS 21

III. REFERENCES 23

CLAIRE C. McCASKILL
Missouri State Auditor

Honorable Bob Holden, Governor
and
Carol Russell Fischer, Director
Department of Revenue
Jefferson City, MO 65102

The State Auditor's Office audited the Department of Revenue's information resource security controls. The objective of this audit was to evaluate whether department officials have established adequate security controls to ensure the integrity, confidentiality, and availability of data and information.

We concluded department officials need to develop and approve a department-wide security framework and plan covering all major facilities and operations. They also need to implement procedures to assess the effectiveness of operational security controls and properly train all personnel with an ongoing security awareness program.

We conducted the audit in accordance with applicable standards contained in *Government Auditing Standards*, issued by the Comptroller General of the United States, and included such tests of the procedures and records as were considered appropriate under the circumstances.

Claire McCaskill
State Auditor

The following auditors contributed to this report:

Director of Audits:	William D. Miller, CIA
Audit Manager:	Jon Halwes, CPA, CGFM
Information Systems Audit Manager:	Jeff Thelen, CPA
In-Charge Auditor:	Tara Shah, CPA
Audit Staff:	Frank Verslues
	Lori Melton, CPA

224 State Capitol • Jefferson City, MO 65101

Truman State Office Building, Room 880 • Jefferson City, MO 65101 • (573) 751-4213 • FAX (573) 751-7984

RESULTS AND RECOMMENDATIONS

1. Controls Over System Access are Weak or Missing

The Department of Revenue (department), which collects taxes and administers drivers' licenses and motor vehicle records, needs to better address system access control management policies and practices. These practices protect the integrity, confidentiality, and availability of data and information, which are at risk from unauthorized use, modification, or disclosure. Current department practices do not:

- Use fully compatible user access management and administration tools.
- Control the number of individuals who can administer access rights to the system applications.
- Have standards for creating, controlling, and monitoring computer access.
- Ensure live production data is adequately protected.
- Properly manage user identifications (IDs).
- Ensure the integrity of staff in highly sensitive positions.

Background

The department has three divisions (Motor Vehicle and Drivers Licensing [motor vehicle], Taxation and Collection [tax], and Administration). Each of these divisions has an administrator of technology services who reports to his/her respective division director. The department also has a chief information officer who handles department-wide issues and works with all the divisions. In September 2001, department officials hired a security coordinator who is assigned department-wide responsibility for internal controls and security policies and procedures. In addition, the State Data Center operates as a data processing and mainframe service provider to the department.

Information resource security access controls provide reasonable assurance that data are protected against unauthorized use, modification, disclosure, loss, or impairment. The purpose of controlling access to data and information is to ensure (1) users have only the access needed to perform their duties, (2) access to very sensitive resources is limited to a few individuals, and (3) employees are restricted from performing incompatible functions or functions beyond their responsibility.

Draft security policies and standards prepared

In August 2001, a department official drafted an information security policies and standards document. In October 2002, this document was taken to the department's Information Security Committee. Approval is expected in 2003. In July 2002, department officials approved a separate department-wide policy covering user ID and password security; however, the information in the policy is very general. The policy also outlines the responsibilities of the chief information officer and the Information Security Committee.

In 1999, the department officials paid International Business Machine (IBM) Global Services about $160,000 to assess the department's security controls. This assessment was designed to

help the department identify potential vulnerabilities in the configuration and management of selected systems, as well as recommend strategies for an effective security program. At least half of the issues in this report were noted in the IBM report, but department efforts have been slow to correct these weaknesses.

See Appendix II, page 21, for key terms and definitions used in the report.

Criteria used to evaluate the department

Currently, no state guidelines exist to establish the need or specific parameters for information resource security controls or security program planning. However, the State Data Center has established a customer procedures manual, which outlines specific policies for state agencies as customers.

In addition, there are federal, national and international standards related to information resource security controls and security program planning. For our review, we used accepted standards from the following sources:

- National Institute of Standards and Technology
- Information Systems Audit and Control Association
- American Institute of Certified Public Accountants
- U.S. General Accounting Office
- Canadian Institute of Chartered Accountants

System access management tools present problems

The department uses two separate ID management systems to administer mainframe access. The two management systems do not interface correctly, which results in many discrepancies in user ID status. These discrepancies place the department at risk of allowing inappropriate access to system resources.

Approximately 2 years ago, the department developed an access management system for administering mainframe access. Prior to the development of the department's system, system administrators could use only the state's mainframe management system to process transactions for user ID mainframe access. The department designed its system as a user-friendly tool for system administrators and to supplement the state's system. Table 1.1 identifies the number of system administrators using the two user ID management tools.

Table 1.1: Management System Administrators

User ID Management System	Number of System Administrators
Department System	20
Statewide System	13
Both Systems	9
Total System Administrators	42

Source: Department system data

Access changes in the department's system will automatically update information in the statewide system, but access changes using the statewide system do not update in the department's system. For example, if one of the 13 administrators, who only uses the statewide system, revokes or resets a user ID, that change will not be reflected in the department's system. The department's system is the primary system used to administer mainframe access. System administrators rely on the status of user IDs in the department's system to monitor user access. As a result of the system interface weakness, we identified:

- 311 active department system IDs that were inactive in the statewide system
- 130 active statewide system IDs that were inactive in the department system

Such discrepancies could result in unknown inappropriate access to system resources.

Access management to computer systems needs improvement

The department has some procedures in place regarding granting access to mainframe applications. The majority of these access procedures are established by each division and are not documented. Department staff told us many of the procedures followed are based on system administrator preferences. Department officials further explained the lack of formalized department-wide security procedures is due to division officials creating their own security procedures and methodologies in the autonomous environment the department operates in.

System and Application Administrators

Number of administrators needs evaluation

As indicated in Table 1.1, there are 42 system administrators. The department has granted four of the system administrators global system rights, which allow them to establish initial access for users, assign user access, and modify and remove access. The other 38 system administrators have the authority to assign and reset user IDs, but cannot assign initial access. Department officials were not aware of the number of employees with system administrator rights prior to our analysis. In addition, officials are not reviewing the necessity of privileged account assignments or ensuring supervisors periodically review the administrators' work. Accepted standards state the number of privileged accounts should be reasonable and based upon the size of the environment.

When an employee has a user ID established and assigned to specific applications, separate application administrators assign rights to the user ID allowing the user to perform specific actions within the application. We compared the number of users for whom division application administrators were responsible. Per Table 1.2, the ratio of application administrator accounts to users is much higher for motor vehicle division applications compared to tax division applications. Department officials could not explain why there are 33 motor vehicle application administrator accounts.

Table 1.2: Comparison of Application Administrators

Application	Administrator Accounts	Application Users	Ratio
All Tax Applications	2	900	1:450
Missouri Titles and Registration	22	800	1:36
Missouri Drivers License	11	200	1:18

Source: Department system data and department personnel

To determine the reasonable number of system and application administrator accounts, department officials should answer the following questions:

- What are the authorized procedures for assigning the administrator privilege?
- Were the administrators' rights which currently exist properly authorized?
- Why does a staff member need the administrator privilege?
- Does the need for such privileges still remain?
- How often does this need arise?
- Can the administrators' needs be handled by restricting their privileges?

Such an assessment will allow department officials to limit the number of privileged accounts to the minimum necessary to manage system and application security.

Formal standards for establishing user access are needed

The department has not established documented policies or standards to provide control over the configuration of user IDs and user groups. When a user's ID is established, there are no formal standards for the system administrator to follow in establishing access. As of August 2002, there were 5,058 active user IDs and 354 user groups. System administrators manage user groups as a convenience for assigning rights to users with similar job duties. However, the user group definitions have not been fully documented. Therefore, department officials cannot ensure the users are being assigned to the appropriate groups. The department also has approximately 1,180 datasets where information is stored and access is restricted. Again, department officials have not documented the information associated with each of these datasets. By not establishing standards controlling the establishment of user and group profiles and defining groups

and datasets, data owners are at risk of being unable to ensure that user access rights are commensurate with user's job responsibilities.

Access rights need to be properly approved

Procedures are not in place to consistently ensure mainframe access is properly approved, which may cause employees and contractors to have unnecessary access to data. For 7 of 13 (54 percent) new employees tested, the department had no documentation of the access request or the employee's supervisor did not approve the access request. Also, access authorization documentation could not be located for all four contractors tested. Motor vehicle system administrators require supervisors requesting access to submit an access request worksheet either by hardcopy or by email. However, those documents are not retained once access is granted. Supervisors in the other two divisions use an electronic request application for approving access, but there are no standard procedures for using the application. Department personnel have not developed procedures nor trained the users on how to properly use the application.

Accepted standards state access needs should be approved by an appropriate senior manager and directly communicated in writing before access is granted. Those approved authorizations should be maintained on file. The following criteria should be defined when granting a user access to a computer system:

- Who is allowed to access or use the component.
- The purpose of the allowed access.
- The duration for which access or use will be granted.
- The type of access permitted.
- Whether the use of the access will be reported and monitored.
- Any other requirements to be applied.

The department is not adequately protecting production data

Computer programmers have access to production data. Supervisors told us the programmers may have to perform special operations from time to time that only they have the rights to do. However, accepted standards state senior management should implement a division of roles and responsibilities to limit the possibility of a single individual subverting a critical process. A segregation of duties should be maintained between functions including data entry and systems development and maintenance. If more complex operations need special rights, those rights can be assigned when necessary and the business function staff could be trained to perform such operations.

Outside contractors' access needs better management

A process is not in place to allow department officials to readily identify all third-party contractors who have access to department system resources and facilities. A centralized list of outside contractors doing business with the department is not maintained. Therefore, there is less assurance only active contractors have appropriate authorized

access to the department's mainframe system and facilities. Accepted standards state management should ensure all third-party contractors' services are properly identified. In addition, since outside contractors are users of the department's data and resources, the same security controls should apply to them as all other employees who have system and facility access.

Access rights not periodically evaluated

82 former employees had active user IDs

The department's mainframe system administration fails to ensure user access rights are appropriate. The department lacks a policy requiring supervisors to periodically reassess employees' access to department information system resources and data. Accepted standards require management to review and confirm access rights periodically to ensure access rights remain commensurate with user job responsibilities. Such reviews also reduce the risk of errors, fraud, misuse or unauthorized alteration.

At August 2002, auditors noted the following problems in the department's mainframe access that would have been identified through periodic reviews of user accounts.

- Eighty-two former employees had active user IDs. Two of these user IDs were for system administrators.

- Six user IDs assigned to contractors were still active, but had not been accessed since November 2000. These contractors are no longer working on mainframe projects for the department.

- At least 14 employees had more than one active user ID. Four of these employees had transferred divisions within the department and the access from the prior division had not been removed. Department personnel stated an employee should not be assigned more than one active user ID.

- Two of the three employees reviewed in detail had more mainframe access than was necessary for their job responsibility. For example, one clerk in the Division of Administration who had supply ordering responsibility also had rights to some motor vehicle and tax applications. She could not perform any function in these applications. The rights may have been left over from a recycled ID.

48 percent of active user IDs not accessed for 180 days or more

In addition to not reviewing access rights, the department's system administrators do not monitor dormant user IDs. At August 2002, 48 percent (2,074 of 4,364) of all active user IDs, which had been used at least once, had not been accessed for 180 days or more. Table 1.3 shows the inactivity timeframe for the user IDs that have not been used for 90 days or more.

Table 1.3: Dormant User IDs

Dormant Period	Number of System IDs
90 days or more	2,137
180 days or more	2,074
1 year or more	1,991
2 years or more	1,793
4 years or more	1,658
8 years or more	161

Source: Department system data

Accepted standards and the department's draft security policies and standards require management to ensure dormant accounts are removed from the system. Periodically monitoring and removing dormant system accounts can reduce the risk of unauthorized access to the department's data.

User IDs need to be properly managed

Department officials are not following State Data Center procedures, accepted password standards, user identification standards, and the department's draft security policies and standards by allowing users to share user IDs and associated passwords and by maintaining user IDs that have not been uniquely assigned to department employees. Changes to users' accounts, data modifications, and the execution of batch processing jobs cannot be readily tracked to the user who performed the function. These situations increase the risk of unauthorized modifications and changes to data, information and user accounts. Department system administrators stated they prefer using shared IDs in some instances because they are easier to administer. Unassigned user IDs are maintained to provide employees with user IDs when needed.

Department data and information are subject to an increased risk of unauthorized loss and use because certain passwords are shared and not appropriately protected. Division of Administration Information Technology Bureau personnel maintain seven user IDs and passwords for shared IDs in four files on the mainframe. The user IDs and passwords are not encrypted but rather are in a readable format and are being shared by all group members. When employees need to access an information resource that requires use of one of these shared IDs and passwords, they read the shared password file to obtain the access information needed. Three of the four password files contained more than one user ID and password. The global system administrator user ID and password is located in two of these shared password files. In addition, eight employees who are not supposed to be acting in the capacity as a system administrator have access to one of the datasets with the global system administrator user ID and password. For example, if an employee had access to one file for one ID and password, he/she would also have access to all other IDs and passwords in that file. The security of a password system is dependent upon keeping passwords secret. Allowing users to share user IDs and passwords for administrative convenience threatens the confidentiality and integrity of the department's data and information.

Not all user IDs maintained by the department are uniquely identifiable using the assigned user name. User IDs provide a method of maintaining accountability, a key to any computer security program. The department maintains over 1,500 mainframe system IDs that have not been assigned to users and 1,612 active shared IDs. This lack of accountability can have an adverse impact on the confidentiality and integrity of data and poses a security risk to the department's information resources.

Unassigned IDs create risk

Department system administrators manage the majority of these 1,500 unassigned IDs in "pools." They created the pools of IDs for the convenience of having pre-established user IDs assigned with basic rights. In addition, the revoked user IDs of terminated employees are returned to the pool, but the access rights associated with the user IDs are not removed before placing the IDs in the pool. By pre-establishing system accounts with basic access rights and leaving rights with other revoked user IDs, department information resources are susceptible to inappropriate use. These IDs may be easily activated and used inappropriately, allowing unauthorized access to system resources. State Data Center procedures and accepted standards require that unique user IDs must be assigned to individual users. All user IDs created should have an associated request and approval that is appropriate for the department's information resources. In addition, user IDs for terminated employees should not be reused but should be revoked or deleted to prevent assigning inappropriate access, which is possible when recycling user IDs.

Background screenings should be re-performed for sensitive job positions

Department officials risk not being able to detect unacceptable employee actions because background screenings are not performed on current employees. Background investigations, which include a Highway Patrol criminal background check, are only performed on applicants being offered a job with the department. Background screenings help determine whether an individual is suitable for a given position. However, similar screenings are not performed when an employee transfers to another position within the department. The new position could be one that a new background screening might find unsuitable for the employee. In addition, accepted standards suggest periodic background reinvestigations should be performed at least once every 5 years, consistent with the sensitivity of the position. However, department officials have not assigned different levels of sensitivity to job positions and have not performed reinvestigations.

Conclusion

Significant weaknesses exist within the department's system access controls. Department officials rely on not fully compatible user ID management systems and have not established effective computer security controls over system administrator and user IDs. Some of these weaknesses are addressed in the department's draft information security policies and standards, which may be finalized in 2003. Poor access management controls may cause users to have access not commensurate with their job function and unauthorized access to department system resources.

Recommendations

We recommend the Director, Department of Revenue:

1.1 Evaluate the usage of the mainframe user ID management systems and implement procedures to eliminate the discrepancies between the systems.

1.2 Evaluate the number of system and application administrators that control access to department data and information system resources. In addition, establish procedures for supervisors to periodically review system and application administrator activity.

1.3 Establish department-wide controls over the configuration of user and group profiles to ensure that access rights for users are commensurate with users' job responsibilities.

1.4 Document and define datasets and ensure only appropriate users have access.

1.5 Ensure policies, procedures, and standards are documented and followed in granting access to data and information system components.

1.6 Ensure the functions of critical processes including that of data entry and systems development and maintenance are properly segregated.

1.7 Ensure a list of contractors with access to department resources and the access given is maintained.

1.8 Ensure supervisors perform documented periodic reviews of user access levels to determine if they remain appropriate.

1.9 Establish policies, procedures, and standards which document the criteria to be followed in closing user accounts and removing access to data and information system resources. These procedures should include policies on monitoring and removing inactive user accounts.

1.10 Establish user groups for users with similar job functions and access rights and discontinue the use of shared IDs and passwords.

1.11 Remove all unassigned user IDs established and formalize procedures to create new IDs upon authorized request.

1.12 Ensure background reinvestigations are performed periodically for applicable employees.

Department of Revenue Responses

1.1 The department agrees that the usage of mainframe user ID management systems should be re-evaluated. The department will re-evaluate the mainframe user ID management systems and review our procedure to ensure that any discrepancies are eliminated. Any procedural changes will be reviewed and approved by the Information Security Committee (ISC) and implemented throughout the department.

1.2 The department agrees that the number of system and application administrators needs to be re-evaluated. Additionally, the department agrees that a procedure needs to be established to formalize the periodic review of system and application administrator activity. The department will review the number of system and application administrators, as well as the periodic review of system and application administrator activity as a function of the ISC. Appropriate procedures will be reviewed and approved by the ISC and implemented throughout the department.

1.3 The department agrees that access rights for users must be commensurate with users' job responsibilities. Appropriate controls will be reviewed and approved by the ISC and implemented throughout the department.

1.4 The department agrees that additional documentation and definition of datasets is required to ensure that appropriate access is provided to users. The department will create the needed documentation and definitions for the datasets.

1.5 The department agrees that a standard procedure must be enforced to ensure that appropriate access is granted to data and information. A working group is currently preparing a draft standard procedure for the request and granting of access to data and information. The draft standard procedure will be reviewed, and, if appropriate, approved by the ISC and implemented throughout the department. The draft standard procedure currently under development will be reviewed at the ISC April 2003 quarterly meeting.

1.6 The department agrees that proper segregation of duties of critical processes is desired. The department will review the duties of personnel associated with data entry, system development, and system maintenance to ensure proper segregation of duties to the extent possible.

1.7 The department agrees that a centralized list of contractors with access to department resources must be maintained. The ISC has approved and forwarded to the Executive Leadership Team for review and approval, a procedure for the Human Resource Services bureau to begin tracking and monitoring contractors with access to department resources.

1.8 The department agrees that periodic reviews of user access must be completed. The department will develop a standard procedure for the periodic review by supervisors to ensure that the appropriate level of system access exists for department personnel. The

draft standard procedure will be reviewed and approved by the ISC, then implemented throughout the department.

1.9 The department agrees that policies and standard procedures must be documented for the removal and review of system access. A working group is currently developing a draft standard procedure. The draft standard procedure will be reviewed and approved by the ISC, then implemented throughout the department.

1.10 The department will review its procedures regarding the use of user IDs and passwords and take this recommendation under advisement.

1.11 The department agrees that procedures for the establishment of new user IDs should be formalized and documented. A working group is currently preparing a draft standard procedure for the creation of new user IDs and granting of access to data and information. The draft standard procedure will be reviewed, and if appropriate, approved by the ISC and implemented throughout the department.

1.12 The department and the Office of Administration will explore the feasibility of conducting reinvestigations for applicable employees.

2. The Department Lacks a Computer Security Management Program

A primary reason for the department's access control weaknesses is the lack of a department-wide computer security management program to ensure computer security receives adequate attention. An effective program would include (1) guidance and procedures for assessing risks, (2) establishing appropriate policies and related controls, (3) raising awareness of risks and mitigating controls, and (4) evaluating the effectiveness of established controls.

Computer security framework needed

Although department divisions have developed security procedures, no formal department-wide security policy existed before July 2002. That limited policy, which is discussed on page 2, does not cover all necessary issues. According to accepted standards, an organization should have a written, up-to-date security policy covering all major facilities and operations agency-wide. Organization policies and procedures should create a framework, giving specific attention to information technology, fostering a positive control environment, and addressing such aspects as:

- Security planning
- Risk management
- Review of security controls
- Life-cycle management
- Authorization for processing
- Personnel
- Physical and environmental aspects
- Computer support and operations
- Contingency planning
- Documentation, training and responses to incidents
- Access controls
- Audit trails

From the framework, the organization's management should develop more detailed guidance or standards that describe an approach for implementing policy. The department's Information Security Committee is currently evaluating a more detailed policies and standards document, which should be finalized in 2003.

Department officials are not currently requiring two specific items essential to security planning (1) classifying data and information into security levels and (2) assigning ownership of the data and information. Data is generally classified into four levels (public, internal, confidential, and classified). State Data Center procedures and accepted standards require data and information classification levels to be established and defined. Data owners should then use the classification levels to identify the security level of their data and the system administrators should follow the access rules for the class type. In addition, department officials have not established any procedures for assigning an owner to data and defining the responsibilities of data owners. The draft security policies and standards address these weaknesses.

The department needs an ongoing computer security awareness and training program

Department officials do not train personnel on an ongoing basis regarding computer security and their role in ensuring appropriate use of department resources. The department's employees play a crucial role in ensuring the security of computer systems and information resources. According to accepted standards, education, training and awareness are all necessary to successfully implement any computer security program. In addition, State Data Center procedures require departments to implement a data security awareness program. Security awareness, training, and education enhance security by improving awareness of the need to protect system resources. Additionally, training develops skills and knowledge so computer users can perform their jobs more securely and build in-depth knowledge. Until recently, the department's computer security training only consisted of a short briefing to new employees on security and control awareness when discussing department usage policies. In August 2002, employees received department-wide confidentiality training which department officials intend to repeat regularly.

Effectiveness of security controls has not been assessed

The department has not implemented processes or procedures for assessing the effectiveness of the current informal security policies. The draft policies and standards which may be finalized in 2003 do not address assessment of policies. Without such an assessment process, there is less assurance the security measures are effective and functioning properly. Accepted standards state periodic self-assessments and independent reviews should be performed to confirm compliance with established policies, procedures, and standards.

Standards for security are available

The Federal Chief Information Officers Council (council) in conjunction with the National Institute of Standards and Technology issued a framework for federal agencies to assess the effectiveness of their computer security programs. The document states adequate security of information and the systems that process it are a fundamental management responsibility. Moreover, management must understand the current status of an organization's security program and controls to make informed judgments that appropriately mitigate risks to an acceptable level. The council's framework security requirements are not new, but are abstracted directly from long-standing requirements found in generally accepted guidance on computer security and privacy. Additionally, the control objectives presented in the framework are generic and can be applied to any organization in the private and public sector.

The computer security assessment framework identifies five levels of computer security program effectiveness, with five being the highest level of security effectiveness. The council stated each federal agency should be at Level 4 striving to get to Level 5. The department's computer security program does not meet the criteria for any of the levels of the framework. According to the council, a Level 1 security program consists of a formally documented program that establishes a continuing, agency-wide cycle of assessing risk; implements effective security policies including training; and promotes monitoring for program effectiveness. As discussed in this report, the department has not developed a formally documented computer security program that contains the elements suggested by the council. The National Institute of Standards and

Technology has issued a self-assessment guide that includes an extensive questionnaire containing several computer security control objectives, which we did not test. This guide is designed for use by those responsible for security at the management, system and organization levels and is electronically available at http://csrc.nist.gov.

Access and security violations are not sufficiently monitored

Department officials have not taken sufficient steps to ensure system security controls are functioning properly. The first step in establishing effective security is developing procedures for logging appropriate security-related events, monitoring specific access, and investigating apparent security violations. Currently, the security administrator receives a weekly report of department-wide mainframe violations for trend analysis and is working on a way to distribute this detail out to appropriate personnel for review. The department has not documented any of these processes. When potential violations are brought to the attention of appropriate officials, procedures are in place to investigate and take necessary action; however, department officials do not routinely review computer system reports, which identify what changes have been made to critical functions, such as computer system security values. Accordingly, unauthorized changes to critical security controls could go undetected. In addition, employee access activity to confidential data is not monitored to detect failed attempts or unusual patterns of successful access to such information. Routinely monitoring the access activities of employees can help identify significant problems and deter employees from inappropriate and unauthorized activities.

A security monitoring program should include (1) identifying sensitive system files, programs, and data files on computer systems and networks, (2) using the audit trail capabilities of security software to document both failed and successful access to these resources, (3) defining normal patterns of access activity, (4) analyzing audit trail information to identify and report on access patterns that differ significantly from defined normal patterns, (5) investigating potential security violations, and (6) taking appropriate action to discipline perpetrators, repair damage, and remedy the control weaknesses that allowed improper access to occur.

Termination policies and procedures need to be enforced

Department procedures may not ensure terminated employees have properly had their access to information system resources and department facilities removed. While department administrative policies require an exit checklist to be completed for all terminated employees, 17 of 28 (61 percent) employees tested did not have a completed employee exit checklist on file. One of these employees still had an active user ID at August 2002. The other IDs had been revoked or reassigned to other employees, but the date this change occurred could not be readily provided by department officials. Department staff stated exit checklists are not completed for dismissed employees or those who die during employment. This checklist guides the supervisor and the human resources personnel through important termination procedures that include:

- Deleting computer identification (including mainframe access and network access)
- Obtaining the employee's identification badge
- Obtaining door and vehicle keys

- Obtaining state credit card
- Obtaining telephone credit card
- Removing employee's name from after-hours access lists, etc.

Without properly completing the exit checklist, it is possible terminated employees may still have access to resources and facilities. Department officials stated the policy regarding the completion of exit checklists will now be enforced for all employees.

Conclusion

The department lacks complete computer security policies and procedures and has limited or no processes for performing effective periodic control assessments or for monitoring and detecting security violations. Department staff do not always follow exit procedures for terminating employees leaving potential unauthorized access to department resources and facilities. In addition, an effective security awareness and training program is not in place. Policies and procedures being evaluated by department officials will address several of these issues.

Recommendations

We recommend the Director, Department of Revenue:

2.1 Complete design, development, and approval of a department-wide security framework and security plan. The security framework should be designed to document and ensure consistent implementation of effective and consistent security practices for all divisions and personnel. Ensure the plan includes:

- A data and information classification framework scheme and guidelines for classifying all data and information in terms of criticality and sensitivity, which is determined by a formal and explicit decision by the data owner.

- A structure for formally appointing data and information resource owners and for defining their roles and responsibilities, which includes making decisions about classification and access rights.

2.2 Implement an ongoing security awareness program to ensure all personnel and end-users are aware of appropriate, department-wide security policies and standards and are informed of their individual responsibilities relative to ensuring a secure processing environment.

2.3 Establish policies and procedures for assessing the effectiveness of operational security controls. Consider using the National Institute of Standards and Technology computer security self-assessment guide to evaluate this effectiveness and make improvements where needed.

2.4 Develop and document department-wide policies and procedures for (1) logging system access, (2) monitoring access and security violations, and (3) reporting to ensure the proper functioning of controls in the department security framework.

2.5 Ensure employee termination policies and procedures are enforced.

Department of Revenue Responses

2.1 The department agrees that a comprehensive information security plan must be developed and approved. The Information Security Manager is working with department personnel, groups, and committees to develop the necessary elements of the department's information security plan.

2.2 The department agrees that implementation of a security awareness program is necessary. Currently, a comprehensive security awareness program is under development by the Information Security Manager. Portions of the program have been implemented. During 2002, every employee of the department participated in a "Confidentiality and Open Records Request" training course. Additional work is underway to provide additional awareness, education, and training to all employees of the department.

2.3 The department agrees that assessment of the effectiveness of operational security controls is vital to the long-term success of any security framework, plan, or program. The department has taken steps to obtain the professional services of outside experts in the assessment of security controls. Additionally, the department will consider different tools, resources, and personnel to assist with an objective assessment of the department's security controls. A comprehensive statewide standard for the assessment of security controls would be beneficial to all state agencies.

2.4 The department agrees that policies and procedures designed to log, monitor, and report system access and violations are necessary to ensure the adequacy of our information security program. The ISC will review and approve appropriate policies and procedures to ensure adequate controls exist.

2.5 On September 27, 2002, a memorandum was sent to all supervisory and management staff with a copy of the department's revised "Exit Checklist" form. Supervisory and management staff were notified that this form is required to be completed for all departing employees, including dismissals, retirees, resignations, and temporary employees.

3. Physical Security Controls are Not Adequate

Computer and other information resource facilities are at risk of being accessed by unauthorized employees and visitors. Unauthorized access can occur because the department does not adequately enforce rules for granting, controlling, and monitoring physical access. Physical access controls are important for protecting the department's computer facilities and resources from damage, theft, and sabotage and are vital to safeguarding the department's critical data and confidential information.

Physical security controls in place do not restrict computer resource access to authorized individuals. Responsibilities for physical security and protection have not been formally assigned or documented, as accepted standards require. During the audit, we noted department visitors are not always properly controlled and physical access to facilities is not always effectively monitored. For rooms open to visitors, department policy requires the use of a sign-in log; however, visitors were not always required to sign the logs. In addition, one room, which receives visitors, does not maintain a log.

Responsibility not formally assigned

Tools available to monitor employee access are not used effectively. Human resource personnel have a database of all employees and their badge type that identifies each employee's physical access rights within department facilities. However, terminated employees are not removed from the database. As a result, there is no current employee listing to sufficiently monitor physical access. Furthermore, the department does not maintain a list of temporary badges that have been issued. Temporary badges may be issued to contractors, department employees that forgot their badges, or visitors. Without recording when a temporary badge has been issued and to whom it was issued, the department cannot identify all individuals who have access to the department facilities and if that access remains necessary and appropriate. In addition, officials do not review the list of employee badges or a list of keys assigned to department employees to ensure access granted remains appropriate.

Conclusion

Due to a lack of discipline towards physical security at department facilities, visitors are not always properly controlled. In addition, the physical access rights of current employees are not monitored periodically. Without enforcement of the existing physical access policies and implementing a periodic review of authorized access, resources are not adequately protected.

Recommendations

We recommend the Director, Department of Revenue:

3.1 Ensure the responsibilities for physical security and protection are clearly defined, documented, and enforced.

3.2 Ensure policies for identifying and monitoring visitors to department facilities are enforced.

3.3 Maintain accurate reports of individuals with physical access to the department's facilities and regularly review those reports to ensure that current employees have appropriate access.

Department of Revenue Responses

3.1 The department agrees that the responsibility for physical security and protection must be clearly defined, documented, and enforced. Currently the responsibility for physical security is informally shared by several different functional groups, all of which are represented in the ISC. The department will work to more clearly define, document, and enforce the responsibility for physical security. The department has identified many desired physical security improvements; however, current lack of funding prevents the department from pursuing implementation.

3.2 The department agrees that the existing policy regarding monitoring visitors must be enforced. The department will take appropriate action to ensure that employees are aware of the existing policy and that persons assigned to work a reception area are trained on this procedure.

3.3 The department agrees accurate reports of physical access to department facilities should be maintained and reviewed. A draft procedure is under development and will be reviewed by the ISC at the January 2003 meeting. The procedure will provide for centralized reporting of all employees' physical access to department facilities. The procedure includes the periodic review by managers to ensure that current employees have appropriate physical access to department facilities.

APPENDIX I

OBJECTIVE, SCOPE AND METHODOLOGY

Objective

The objective of this audit was to evaluate whether department officials have established adequate security controls to ensure the integrity, confidentiality, and availability of data and information.

Scope and Methodology

Auditors conducted fieldwork during May through September 2002. The audit included:

- Review of applicable federal, national, and international standards related to information resource and physical security controls.
- Discussion with department personnel involved in information resource and physical security controls.
- Review of department records related to information resources and physical access to department facilities and resources.
- Analysis of user ID information for access to the mainframe system.
- Observation of the department's adherence to physical security policies.
- Evaluation of management controls pertinent to information resource security.

The audit reviewed the department's practices and procedures for information resource and physical security controls except for activities that are the responsibility of the State Data Center. Therefore, our audit did not review the security controls of the State Data Center related to the department. Because the objective of our review was to assess the overall effectiveness of the department's security and access controls, we did not fully evaluate all computer controls and we did not perform any penetration testing. System access audit work was concentrated on the mainframe system.

During the audit, we provided department officials with specific detail on security concerns noted for their immediate consideration.

APPENDIX II

DEFINITION OF TERMS

Some key terms and definitions accepted by the organizations noted on page 3 that have developed national and international standards for computer security include:

Access Control: Controls designed to protect computer resources from unauthorized modification, loss, or disclosure. Access controls include both physical access controls, which limit access to facilities and associated hardware, and logical controls, which prevent or detect unauthorized access to sensitive data and programs that are stored or transmitted electronically.

Application: Any of a class of "programs" or "software," which causes a computer to perform some useful function such as data entry, update or query.

Dataset: A data file or collection of interrelated data. The term is used in a mainframe environment, whereas file is used almost everywhere else.

Encryption: The transformation of data from the original, plaintext format to a difficult-to-interpret format as a mechanism for protecting its confidentiality, integrity, and authenticity.

Framework: An outline of the issues that need to be addressed in a comprehensive department-wide computer security plan. Provides background and rationale for information technology security, evaluation, certification and system accreditation. It is intended to be used at management level.

Information Resource: All computer-related activities involving any device capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, and network environments. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

Mainframe: A multi-user computer designed to meet the computing needs of a large organization.

Physical Security Controls: Controls such as locks, guards, badges, alarms, and similar measures (used alone or in combination) that help to safeguard computer facilities and resources from intentional or unintentional loss or impairment by limiting access to the buildings and rooms where they are housed.

Production data: The data that supports an agency's operational information processing activities. It is maintained in the production environment as opposed to the test environment.

Production environment: The system environment where the agency performs its operational information processing activities.

APPENDIX II

Profile: Data that describes the nature and extent of system access for a user, a group of users, or one or more computer resources.

Security Administrator: The person(s) responsible for managing the security for computer facilities, computer systems and/or data that is stored on computer systems or transmitted via computer networks.

System Administrator: The person(s) responsible for administering use of a multi-user computer system, communications system, or both.

APPENDIX III

REFERENCES

American Institute of Certified Public Accountants

AICPA/CICA SysTrust: Principles and Criteria for Systems Reliability, Version 2.0, January 2001.

Auerbach Publishers

Information Technology Control and Audit, Frederick Gallegos, Daniel P. Manson and Sandra Allen-Senft, 1999.

Standard for Auditing Computer Applications, Martin A. Krist, 1999.

Canadian Institute of Chartered Accountants

Information Technology Control Guidelines 3rd Edition, July 1998.

Federal Chief Information Officers Council

Federal Information Technology Security Assessment Framework, November 28, 2000, http://www.cio.gov.

Information Systems Audit and Control Foundation

Control Objectives for Information and Related Technology (COBIT), 3rd Edition, July 2000, http://www.isaca.org.

Certified Information Systems Auditor (CISA) Review Manual, 2002, http://www.isaca.org.

Missouri Office of Administration - Division of Information Systems State Data Center

Customer Procedures Manual, Section IX, January 2002.

National Institute of Standards and Technology

Special Publication 800-12, *An Introduction to Computer Security: The NIST Handbook,* October 1995, http://csrc.nist.gov.

Special Publication 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems,* September 1996, http://csrc.nist.gov.

Special Publication 800-18, *Guide For Developing Security Plans For Information Technology Systems,* December 1998, http://csrc.nist.gov.

Special Publication 800-26, *Security Self-Assessment Guide For Information Technology Systems,* November 2001, http://csrc.nist.gov.

U.S. Office of Management and Budget

Appendix III to OMB Circular No. A-130, *Security of Federal Automated Information Resources*, November 2000, http://www.whitehouse.gov/omb/circulars/index.html.

U.S. General Accounting Office

Federal Information System Controls Audit Manual: GAO/AIMD-12.19.6, January 1999, http://www.gao.gov.

Warren Gorham & Lamont/RIA Group

Handbook of IT Auditing, 2001 Edition.