Susan Montee, CPA
Missouri State Auditor

October 2007

LABOR AND INDUSTRIAL RELATIONS

Workers' Compensation Data Security Controls

Report no. 2007-61

auditor.mo.gov

Susan Montee, CPA
Missouri State Auditor

YELLOW SHEET

Missing Security Controls Leave Confidential Data and Technology Resources Susceptible to Unauthorized Access

This audit reviewed the management and control of information technology resources at the Department of Labor and Industrial Relations (DOLIR) Division of Workers' Compensation (DWC). Auditors found DOLIR and Information Technology Services Division (ITSD) management have not taken some of the measures necessary to maintain effective controls to protect the confidentiality, integrity and availability of data and the information technology resources supporting the mission and operations of DWC.

User account administration needs improvement	DOLIR's user account administration procedures lack key security control requirements commonly recommended by accepted standards. DOLIR and ITSD management have not implemented policies and procedures for periodically reviewing user access rights to the network or to DWC information systems and application data to ensure access rights remain appropriate. As a result, users have access to functions outside of the users' job duties, programmers have access to production data, and user account administration policies have not been developed. According to accepted standards, effective administration of users' computer access is essential to maintaining system security. (See page 6)
Physical security access controls have been inadequate	DOLIR and ITSD management have not established adequate policies and procedures for the physical security of DOLIR computer facilities. Auditors found oversight responsibilities for physical security have not been formally assigned and access to facilities has not always been properly controlled or monitored. As a result, access to the computer room has been provided to people who did not require the access levels issued based on their job titles, electronic door access card records have not always been updated when cards have been reissued, access to some secure locations has not been monitored, and a list of personnel authorized to access the offsite storage facility has not been maintained. (See page 9)
Some security controls need to be fully developed	DOLIR and ITSD management have developed and documented policies for specific security controls. However, management has not completed the process of establishing and documenting policies and procedures for some key security controls. Accepted standards state policies are necessary to set organizational strategic directions for security and assign resources for the implementation of security. (See page 11)

All reports are available on our website: auditor.mo.gov

Contents

Abbreviations

AICS	Automated Integrated Claim System
DOLIR	Department of Labor and Industrial Relations
DWC	Division of Workers' Compensation
GAO	Government Accountability Office
ITSD	Information Technology Services Division
MAEA	Missouri Adaptive Enterprise Architecture
OA	Office of Administration
RSMo	Missouri Revised Statutes

SUSAN MONTEE, CPA
Missouri State Auditor

Honorable Matt Blunt, Governor
and
Omar Davis, Director
Department of Labor and Industrial Relations
and
Dan Ross, Chief Information Officer
Office of Administration, Information Technology Services Division
Jefferson City, MO 65102

The Department of Labor and Industrial Relations (DOLIR) Division of Workers' Compensation (DWC) is responsible for working with employers and employees regarding workplace injuries and illnesses. The purpose of workers' compensation insurance is to provide financial assistance to workers injured on the job. The Office of Administration Information Technology Services Division (ITSD) is responsible for providing technical assistance to support DOLIR's technology resources. Our objective included determining whether DOLIR and ITSD management established adequate internal control policies and procedures and implemented effective security controls to ensure the confidentiality, integrity and availability of data and information collected and maintained by DWC.

DOLIR and ITSD management have not taken some of the measures necessary to maintain effective controls to protect the confidentiality, integrity and availability of data and the information and technology resources supporting the mission and operations of DWC. DOLIR management has not adequately reviewed or monitored user access rights which could allow inappropriate access to payment processing functions. DOLIR and ITSD have physical security access controls in place to help protect data and information technology resources from unauthorized access. However, management lacks assurance the controls have been working effectively since policies or procedures for reviewing and monitoring physical access controls have not been established or documented. We also found instances where security policies have not been developed and instances where procedures have been in place but the corresponding policies have not been documented.

We conducted our audit in accordance with applicable standards contained in *Government Auditing Standards*, issued by the Comptroller General of the United States, and included such procedures as we considered necessary in the circumstances. This report was prepared under the direction of John Blattel. Key contributors to this report included Jeff Thelen, Jeff Roberts, Lori Melton, Frank Verslues, and Evans Owala.

Susan Montee, CPA
State Auditor

Introduction

The mission of the Department of Labor and Industrial Relations (DOLIR) is to promote economic security, promote safe and healthy workplaces, and protect wage earners and individuals against discrimination, according to the department's web site.[1] DOLIR employs about 950 persons who provide services to current and emerging businesses and to workers of Missouri. According to the division's web site,[2] the Division of Workers' Compensation (DWC) works with employers and employees regarding workplace injuries and illnesses. State law[3] requires many Missouri employers to carry workers' compensation insurance for employees. The purpose of workers' compensation insurance is to provide financial assistance to workers injured on the job. The DWC also provides mediation services to help employers and employees resolve disputes about medical treatment and lost wages.

The DWC uses the Automated Integrated Claim System (AICS) to process all documents and information pertaining to an injury and for storing and reporting data. Any injury which requires medical aid, other than immediate first aid with no lost time from employment, is required to be reported to the DWC by the insurance company, third-party administrator, or self insured employer using the first report of injury form. About 95 percent of these forms are submitted to the DWC electronically with the remaining 5 percent submitted on paper forms. The DWC received about 133,000 first report of injury forms in fiscal year 2007.

If an employee cannot resolve benefit problems with the employer or with the employer's insurance company, the employee may file a formal claim for compensation with the DWC. Claim forms are submitted on paper forms and entered in AICS by DWC personnel. By filing a claim, the employee begins an administrative law proceeding where an administrative law judge has the authority to decide issues in dispute. The DWC received about 28,000 claim forms in fiscal year 2007.

AICS maintains confidential data including social security numbers and injury information. AICS includes other system areas, such as Medical Services, Image Processing, File Tracking/Archives, Mediations, and Second Injury Fund.

[1] "About Us," *Department of Labor and Industrial Relations*, <http://www.dolir.missouri.gov/aboutus.htm>, accessed July 20, 2007.
[2] "Division of Workers' Compensation," *Department of Labor and Industrial Relations*, <http://www.dolir.missouri.gov/wc/>, accessed July 24, 2007.
[3] Workers' compensation laws are in Chapter 287, RSMo.

The DWC is also responsible for processing Second Injury Fund benefits. The Second Injury Fund compensates injured employees when a current work-related injury combines with a prior disability to create an increased combined disability. When an employee is eligible for benefits and a compromise settlement has been approved or an award has been issued, DWC processes payments to injured workers using AICS. In fiscal year 2007, DWC staff processed about $66 million in Second Injury Fund payments through AICS.

The Office of Administration, Information Technology Services Division (OA ITSD)[4] is responsible for providing technical assistance to support DOLIR's technology resources. DOLIR maintains ownership of its information systems and data, while ITSD provides the technical support. As part of the technology support function, OA ITSD has established the Missouri Adaptive Enterprise Architecture (MAEA)[5] to guide information technology decisions. DOLIR is required to follow MAEA standards and policies.

DOLIR and ITSD share the responsibility for managing security of data and information maintained by DWC. According to accepted standards, security controls are the management, operational, and technical safeguards or countermeasures prescribed for an information system[6] 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 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. According to DOLIR policies, most data obtained by the department is considered sensitive in nature and has restrictive release requirements.

[4] In this report, OA ITSD refers to the entire division, while ITSD refers to the section within OA ITSD that has been assigned specific responsibility for supporting DOLIR technology resources.

[5] The Enterprise Architecture includes standards, policies and guidelines established by OA ITSD. 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.

[6] National Institute for Standards and Technology (NIST), Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*, February 2005, defines an information system as a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Scope and Methodology

To determine whether DOLIR and ITSD management established internal control policies and procedures and implemented security controls, we conducted interviews with appropriate officials and staff; requested and reviewed available policies, procedures, and other applicable information; and performed testing.

We obtained data files from ITSD of user accounts having access to DOLIR's network as of February 2007, and of user accounts having access to AICS as of March 2007. We did not rely on the user account data to draw overall conclusions. Rather, we assessed specific department policies and controls, including controls specific to AICS, and did not perform specific procedures to determine data validity. To help ensure completeness of the data, we grouped the network accounts by division and compared the listing to the DOLIR organization chart and reviewed the AICS accounts for reasonableness and scanned for the names of employees.

We obtained a list from DOLIR management of all persons assigned active security cards able to access the DOLIR computer facility and the building housing the computer facility as of March 2007. This list also included each card holder's access levels. To determine whether assigned access to the computer facility was appropriate, we manually verified where each of the security card holders worked by checking employment records in the statewide accounting system for human resources or by locating the card holder's name on DOLIR's organization chart.

We based our evaluation 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 (MAEA)
- National Institute of Standards and Technology (NIST)
- U.S. Government Accountability Office (GAO)
- IT Governance Institute Control Objectives for Information and related Technology (COBIT)
- International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC)
- Information Security Forum Standard of Good Practice for Information Security

We requested comments on a draft of our report from the Director of the Department of Labor and Industrial Relations and the Chief Information Officer. We conducted our work between February and July 2007.

Missing Security Controls Leave Confidential Data and Technology Resources Susceptible to Unauthorized Access

DWC data and DOLIR information technology resources are susceptible to unauthorized access, use or disclosure. This situation has occurred because DOLIR and ITSD management have not (1) established adequate user account administration procedures, (2) established adequate policies and procedures for physical security, and (3) documented or implemented some key policies and procedures for internal controls, including security. Collectively, these weaknesses impair DOLIR's ability to ensure the confidentiality, integrity, and availability of data collected and maintained by DWC and to ensure information technology resources are properly protected.

User Account Administration Needs Improvement

According to accepted standards, effective administration of users' computer access is essential to maintaining system security. We found DOLIR's user account administration procedures lack key security control requirements commonly recommended by accepted standards. Specifically, DOLIR and ITSD management have not established or fully documented the following user account administration controls:

- User account reviews
- Limiting programmer access to production data
- Access to and security of the Second Injury Fund databases
- AICS user account administration

Informal user account reviews have not been adequate

DOLIR and ITSD management have not implemented policies and procedures for periodically reviewing user access rights to the network or to DWC information systems and application data to ensure access rights remain appropriate. According to the MAEA, agencies must periodically review user accounts. At a minimum, this review should include (1) levels of authorized access for each user and (2) identification of inactive, idle or orphaned accounts. Accepted standards also support regular review of all accounts and related privileges.

The ITSD network administrator occasionally sends out a listing of employee access rights to supervisors for review, according to an ITSD official. However, we found this process has not constituted a comprehensive review of user access to data and other information resources on the network and no documentation exists that supervisors' responses have been used to adjust user access rights. ITSD officials also provide quarterly reports to the DOLIR Security Administrator for verifying network user accounts but these reports have not included the information necessary to allow for a proper review or confirmation of user access rights. According to an ITSD official, AICS user access lists had been provided annually to DWC unit supervisors to review. However, the ITSD official could not provide the date of the last DWC review.

We performed a limited review of user access rights to the DOLIR network and to AICS. We did not find any problems with user access rights to the network. We did however, find four employees who had more than one AICS user account. According to an ITSD official, these employees had been assigned a new user account when transferring to another division, but the old accounts had not been deleted. We also found DWC supervisors did not know six employees had unnecessary access to the AICS delete and payment functions.

Without having documented policies and procedures and a process for reviewing and following up on users' access to data and information resources, management does not have reasonable assurance access rights remain commensurate with user's job duties and responsibilities resulting in an increased risk of inappropriate access.

Programmers have full access to production data

AICS application programmers have access to the computer system data and production environment, including access to Second Injury Fund payment processing functions. According to the MAEA, separation of duties provides process integrity while maintaining proper security and quality controls and must be established and documented so an individual does not have access to more than one critical task. Inadequately segregated duties increase the risk that erroneous or fraudulent transactions could be processed, improper program changes implemented, or computer resources damaged or destroyed, according to GAO.

During our review of AICS user access, we found eight ITSD programmers have administrator rights as well as access to the AICS Second Injury Fund payment processing functions. An ITSD official said the programmers have administrator rights so they can change user access rights, including their own access rights. The official further explained programmers use this ability to change their access rights to mimic another user's rights when providing end user support. By having this capability, these programmers have access to all AICS menu options and all special access menus. In addition, no monitoring or periodic review of the programmers' activities has been performed, according to an ITSD official. Although necessary, temporary access authorizations outside of the normal scope of a user's duties should be granted sparingly and monitored carefully, consistent with the need to maintain separation of duties for internal control purposes, according to accepted standards.

Access to and security of the Second Injury Fund databases needs to be strengthened

ITSD officials have not fully secured the databases used to track the receipt of monies for the Second Injury Fund. The Second Injury Fund surcharge collection databases are used to track, bill and receipt monies collected from insurance companies and self-insured businesses operating in Missouri. At least 16 employees had access to the collection databases, including 8 application programming staff. However, only one employee has been responsible for data entry and tracking of collections, according to a DWC official. Accepted standards state user access rights to systems and data should be in line with defined and documented business needs and job requirements.

ITSD staff said the databases had been developed in 2003 under a tight deadline due to a memorandum of understanding, which transferred the responsibility for collecting Second Injury Fund surcharges from the Department of Insurance to DWC. As a result, common security features had not been included in the databases. Security must be considered in the design of an information system according to accepted standards. Experience has shown it is very difficult to implement security measures properly and successfully after a system has been developed so these measures should be integrated fully into the design and development of the system, according to accepted standards. ITSD officials said a new database is being developed that will be part of AICS and the necessary security features will be incorporated. This new database, including additional security features, should be implemented by December 2007, according to ITSD officials.

User account administration policies and procedures need to be documented

ITSD officials have not documented the controls for the configuration of group profiles or for the authorization, ownership, and use of privileged accounts. These policies and procedures are necessary to ensure system administrators are familiar with the procedures for adding, changing or removing group profiles and are knowledgeable of the requirements for processing changes to user profiles, according to accepted standards. In addition, controls over privileged user accounts should be documented for the proper oversight of security administration staff.

Although ITSD officials have implemented user account administration policies and procedures, the policies have not been fully documented. An ITSD official said management had not been aware the administrative account policies and procedures needed to be documented. Without adequate documentation, DOLIR and ITSD management cannot assure system administration staff are knowledgeable of requirements for providing consistent AICS user account support and control over privileged user accounts.

Physical Security Access Controls Have Been Inadequate

DOLIR and ITSD management have not established adequate policies and procedures for the physical security of DOLIR computer facilities. Specifically, we found oversight responsibilities for physical security had not been formally assigned and access to facilities has not always been properly controlled or monitored.

Management should define and implement procedures to grant, limit and revoke access to premises, buildings and areas according to business needs, including emergencies, according to accepted standards. Access to premises, buildings and areas should be justified, authorized, logged and monitored. This applies to all persons entering the premises, including staff, temporary staff, clients, vendors, visitors or any other third party, according to accepted standards.

Physical security oversight has not been adequate

The MAEA states responsibility for the physical and environmental security program needs to be formally assigned. Appropriate policies and procedures for physical security policies had not been documented and the responsibility for physical security had not been formally assigned to specific ITSD staff. Prior to the start of our audit, responsibility for monitoring physical access of the computer facility and overall responsibility for physical security had not been formally assigned, according to an ITSD official. During audit fieldwork, responsibility for physical security of the ITSD work area was assigned to an ITSD official. We found the following physical security issues at DOLIR that could have been prevented with adequate oversight:

- About 50 electronic door access cards, allowing 24 hours a day, 7 days a week access to the computer room, had been issued to people who did not require this level of access based on their job titles, according to an ITSD official.
- Cardholder records have not always been updated when cards have been reissued. We identified five cardholder records for terminated employees. A DOLIR official said the cards had been issued to new employees without updating the records. In addition, we found 10 card numbers where the cardholder records identified two different people in possession of the same card number.
- There are 103 different types of access levels, however, only 41 levels have been in use. An ITSD official said the number of access levels needs to be reduced to adequately review users' physical access.

Access to information technology resources has not been monitored

DOLIR policy states all staff not authorized for entry to the ITSD work area must sign a visitor's register before entering. However, contrary to this policy, we found the doors to the ITSD work area are only locked from 6:00 pm. to 7:00 am. During work hours, access to these doors has not been monitored and visitors have not been required to sign in.

The door to the computer room is locked and a computerized system is used for logging employee access. However, ITSD officials have not maintained an up-to-date visitor logbook to track visitors and consultants who have been in and out of the room. During a physical walk-through of the computer room in March 2007, we observed a visitor log book that had not been used since July 2006. An ITSD official said ITSD does not have any documented policies and procedures for temporary access by visitors to sensitive areas.

The MAEA requires agencies to create a physical security program. This program should ensure access to critical areas is controlled with door locks; guards or receptionists supervise the movement of people and materials; and administrative procedures, such as sign-in logs, identification cards or badges are in place. The MAEA further requires that visitors be properly controlled and escorted and a visitor's log should be kept and reviewed regularly.

Without documented policies and procedures on physical security access control, DOLIR and ITSD management cannot ensure adequate physical security controls are in place to restrict access to computer resources to only appropriate individuals.

Data stored offsite has not been adequately protected

ITSD officials did not have adequate controls to limit physical access to the offsite facility where backup media are stored. In addition, an offsite storage inventory log has not been kept up-to-date. An ITSD official said the responsibility for monitoring physical security at the offsite storage facility has not been assigned. As a result, critical backup resources have not been adequately protected from risk of loss either thorough purposeful or unintentional activities.

ITSD officials have not maintained a list of personnel authorized to access the offsite storage facility. An ITSD official said only four ITSD employees and one DOLIR employee should have access to this facility. However, during our audit, we were granted access to the facility by an additional DOLIR employee. There is no computerized system, such as a key card, in use to automatically log who enters the offsite storage facility. While this control weakness is not significant, it does place increased importance on

the adequacy of management's control policies and procedures over the distribution of door keys.

According to accepted standards, an organization should develop and keep current lists of personnel with authorized access to facilities containing information systems. The standards also require that designated officials within the organization review and approve the access list.

Inventory logs of the backup media sent to, and received from, the offsite storage facility are maintained in the DOLIR computer room. However, in May 2007, we found one of the inventory logs had not been updated for approximately 2 months. An up-to-date inventory log is necessary to provide proper controls over media stored offsite, according to accepted standards.

Without adequate physical and administrative controls, ITSD officials cannot assure the physical safety of the backup materials stored at the offsite facility.

Some Security Controls Need to be Fully Developed

A security program provides a framework for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of an agency's security controls. According to GAO, implementing a security program is essential to ensuring controls over information and information systems operate effectively on a continuing basis.

DOLIR and ITSD management have developed and documented policies for specific security controls. However, officials have not completed the process of establishing and documenting policies and procedures for some key security controls. Accepted standards state policies are necessary to set organizational strategic directions for security and assign resources for the implementation of security.

DOLIR and ITSD management have not established or documented policies or procedures for the following security controls:

- Data and information ownership
- System and data classification
- Security logging and monitoring
- Backup and offsite storage tests
- AICS user manual
- Data output

Data and information owners need to be formally documented

DOLIR management has appointed information owners who make decisions about data classification and system access rights. However, policies have not been documented regarding the identification of data and system resource owners and a listing of the owners has not been provided to ITSD. A list of information owners is needed to ensure requests ITSD receives for user access changes have been approved by appropriate DOLIR officials.

The MAEA states information owners are necessary to administer information security. It is important to document the ownership of data and information systems because owners make decisions about classifying and protecting information and systems, according to accepted standards. Without having documented policies and procedures establishing data and information ownership responsibilities, there is an increased risk data and information assets will not be properly protected against unauthorized access.

Systems and data have not been classified according to sensitivity and criticality

DOLIR management does not have assurance that information systems and data receive an appropriate level of protection. DOLIR and ITSD management have not established a framework for systems and data classification. The department's information security policy requires a systems and data classification framework. Such a framework examines the sensitivity of both the data to be processed and the system itself to identify when to classify information as confidential, public, or other established levels, according to accepted standards.

According to DOLIR policy, a framework for data and system classification should be established which promotes the integrity, confidentially, accountability, and availability of information. Also, accepted standards provide that a classification framework should include details about data ownership, definition of appropriate security levels and protection controls, and a brief description of data retention and destruction requirements, criticality and sensitivity. An ITSD official said ITSD would adopt a classification framework for DOLIR resources after one is formally incorporated into the MAEA. A draft technology standard on data classification has been issued by OA ITSD, but the standard had not been finalized as of July 2007.

Policies needed to log, report and review security activity

DOLIR management has not taken sufficient steps to ensure system security controls have functioned properly. Policies and procedures for logging appropriate security-related events and monitoring specific access are necessary when developing effective security programs. Accepted standards state a logging and monitoring function enables the early detection of

unusual or abnormal security activity[7] that may need to be addressed to ensure the approved security level is maintained.

System security logging is available on the DOLIR network to identify security events. However, policies and procedures for monitoring, reviewing and investigating the logs have not been established. ITSD officials said DOLIR does not have the resources available to log and monitor security-related events. A survey performed in 2005[8] stated proactive monitoring of system logs might facilitate detection of an incident before it becomes apparent externally. The survey also stated that automated processes for monitoring suspicious activity may be the most effective means of detection.

Determining what, when, and by whom specific actions have been taken on a system is crucial to establishing individual accountability, investigating security violations, and monitoring compliance with security policies, according to GAO.

No periodic test of backup data performed

ITSD officials have established policies and procedures for the backup and off-site storage of critical system data to meet the business continuity strategy of DOLIR. However, this policy does not address periodic tests of the offsite backup data. An ITSD official said files and folders have been successfully restored from backups, which management believes indicates the reliability of the backups. However, accepted standards state organizations should test backup information at an organization-defined frequency to ensure media reliability and information integrity. Without testing the full backups, management cannot be assured the entire system can be restored when necessary.

AICS user manual has not been documented

DOLIR management cannot ensure AICS users have adequate knowledge to allow effective and efficient use of the system to support DWC's business processes. A user or training manual explaining system data input, error handling and processing procedures has not been maintained. A DWC officialsaid employees receive training for AICS on the job and a formal training manual has not been needed. However, accepted standards state

[7] Security activity includes users attempting to access data they are not authorized to access, performing a task they are not authorized to perform, or accessing data they are authorized to access that is of a sensitive nature.

[8] "Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors", *United States Secret Service, National Threat Assessment Center and CERT® Program, Software Engineering Institute at Carnegie Mellon University*, <http://www.cert.org/insider_threat/insidercross.html>, accessed July 9, 2007.

manuals for users should be documented to ensure the proper use and operations of applications.

ITSD officials have also not documented the transaction processing edits incorporated into AICS. An ITSD official said the edits are documented in the source code and there has never been a reason to formally document the edits separately. Without documentation of the edits, DOLIR management cannot ensure users understand and properly use the edits. This weakness reduces management assurance transactions are processed as intended impacting the ability to provide reliable and consistent information.

Policies needed to ensure application output is complete and accurate

DWC management has limited assurance data and reports from AICS are complete or accurate. The policies and procedures needed to provide this assurance have not been documented. An ITSD official said ITSD staff verify output to ensure requests have been processed correctly. This process includes verifying the criteria used for processing agrees to the criteria submitted by DWC and that record counts are complete. DWC officials have also established informal procedures for verifying the completeness and accuracy of special requests, according to DWC staff.

Documented policies and procedures should be established to assure the provider and relevant users review the accuracy of output reports and to ensure the processing of stored information is correct and appropriate to the circumstances, according to accepted standards.

Conclusions

DOLIR and ITSD management have not taken necessary steps to fully implement effective internal control policies and procedures and effective security controls to prevent the unauthorized access, use and disclosure of data. DOLIR management does not have assurance access to data and other information resources is appropriate because user account access has not been adequately monitored or reviewed. ITSD management does not have assurance the DOLIR computer facilities are adequately secured because oversight responsibilities had not been formally assigned and access to facilities has not always been properly controlled or monitored. DOLIR's control environment is missing important security components because management has not documented policies and procedures for some key security controls. Faced with the challenge of protecting systems and resources from continuing threats, vulnerabilities, and data breaches, DOLIR and ITSD management should support establishing and documenting the controls necessary to ensure the confidentiality, integrity, and availability of data and information collected and maintained by DWC.

Recommendations

We recommend the Department of Labor and Industrial Relations management work with Information Technology Services Division officials to:

2.1 Ensure user account administration is fully documented and access is granted appropriately. At a minimum, management should implement user access reviews and document policies and procedures by taking the following actions:

- Ensure supervisors review user access rights and notify ITSD if changes are necessary.
- Establish and document policies and procedures to ensure adequate segregation of incompatible duties. These policies and procedures should limit programmer access to the production environment to temporary situations and ensure activity performed by programmers is periodically monitored.
- Limit access to the Second Injury Fund databases to only those staff that require access as part of their regularly assigned duties.
- Document the controls in place over the configuration of group profiles and the authorization, ownership and use of privileged accounts.

2.2 Establish policies and procedures regarding the physical security of computer facilities. At a minimum, management should implement controls and document policies and procedures by taking the following actions:

- Perform a comprehensive review of cardholder records to ensure access is granted consistent with the assigned duties and responsibilities of the cardholder. In addition, review access levels and delete unnecessary levels to simplify security administration.
- Ensure the established physical security policy is upheld and access is limited to the ITSD work area. In addition, maintain an up-to-date log of visitors who enter the computer facility.
- Protect critical backup resources from the risk of loss by maintaining both a current list of personnel authorized to access the offsite storage facility and a current inventory of offsite backup media.

2.3 Ensure policies and procedures are established and documented for all key security controls. At a minimum, management should implement controls and document policies and procedures by taking the following actions:

- Document the appointed owners who makes decisions about data classification and access rights for all information resources (data and systems).
- Establish a system and data classification framework to ensure all systems and data are classified in terms of criticality and sensitivity.
- Establish and document policies and procedures to log, monitor, report, and review appropriate security activity and security violations.
- Establish and document policies to periodically test backup data to ensure media reliability and information integrity.
- Document a user manual for AICS to ensure the proper use and operations of applications. This manual should include descriptions of the transaction edits available.
- Document policies and procedures required to validate data output to ensure data has been processed and reported completely and accurately.

Agency Comments

2.1

- *DOLIR concurs with the recommendation and will establish procedures for supervisors to monitor and determine on a scheduled basis access rights for users of the AICS.*
- *ITSD-DOLIR concurs with the recommendation and will comply by establishing documented policies and procedures to adequately segregate and limit programmer access to the production environment of the AICS.*
- *DOLIR concurs with the recommendation and has taken steps to determine what staff should have "Modify Authority Only" and who should have "View Copy Only" authority to the Second Injury Fund database. ITSD-DOLIR concurs with the recommendation and will comply by limiting access to the Second Injury Fund Access database to staff who maintains the database as part of her/his assigned duties.*
- *ITSD-DOLIR concurs with the recommendation and will comply by establishing documented policies and procedures for the configuration of group profiles and privileged user accounts.*

2.2

- *ITSD-DOLIR concurs with the recommendation and will comply by conducting internal reviews of cardholder (ITSD and non-ITSD staff) access to ITSD workspace to include the computer room. Additionally, ITSD-DOLIR will limit/simplify the number of access levels.*
- *ITSD-DOLIR concurs with the recommendation and will comply by establishing documented policies and procedures to limit access to ITSD-DOLIR workspace. The policies will include assigning an*

ITSD-DOLIR staff responsibility for physical security and logging of visitors who enter ITSD-DOLIR workspace(s).

- *ITSD-DOLIR concurs with the recommendation and will comply by establishing documented policies and procedures to address offsite backup storage. The policies will address authorization by personnel to offsite storage and the inventory of offsite backup media.*

2.3

- *DOLIR concurs with the recommendation and will determine information owners responsible for making decisions about data classification and system access rights and provide such list to ITSD-DOLIR to ensure that user access changes are appropriately approved.*
- *DOLIR concurs with the recommendation and will work with ITSD-DOLIR to determine the most appropriate policy based on accepted standards to classify information and to promote the integrity, confidentiality, accountability and availability of information in the AICS. DOLIR will implement the appropriate policy in a timely manner.*
- *ITSD-DOLIR concurs with the recommendation and will comply by establishing documented policies and procedures to log, monitor and report appropriate activities and security violations.*
- *ITSD-DOLIR concurs with the recommendation and will comply by evaluating the technical aspects of this type of testing and determine the internal and external costs. Once costs are determined, ITSD-DOLIR will seek funding to conduct the testing on a regular basis. Once funding is secured, a policy will be developed and implemented. This testing must be performed in a way to not disrupt the ongoing production work of any systems.*
- *DOLIR concurs with the recommendation and will develop an AICS user manual that will allow efficient and effective use of the AICS and will support business processes. Notwithstanding the need to ensure proper use of AICS applications, DOLIR must also consider that the DWC is planning to either make significant changes to the AICS or replace the AICS system altogether in the near future. Therefore, DOLIR must examine the cost effectiveness of developing a user manual for the current AICS or waiting to develop a user manual for any system that is developed.*
- *DOLIR concurs with the recommendation and will document, using accepted standards, the policies and procedures that are currently used to assure data and reports from the AICS are complete and accurate.*