Office of Missouri State Auditor

Nicole Galloway, CPA

Unemployment Insurance System Data Security

Report No. 2019-008
February 2019

auditor.mo.gov

Nicole Galloway, CPA
Missouri State Auditor

CITIZENS SUMMARY

Findings in the audit of the DOLIR Unemployment Insurance System Data Security

User Account Management

Department of Labor and Industrial Relations (DOLIR) management has not fully established controls for the maintenance of user accounts for accessing the UInteract system. Established controls (1) disable a user account when the account has not been accessed for 120 days and (2) limit access to system administrative functions to computers attached to the state's internal network. However, the quarterly review process used by the DOLIR to detect and remove terminated user accounts did not effectively identify all accounts belonging to users not employed by the DOLIR. DOLIR management could reduce the risk of unauthorized access by increasing efforts to identify user accounts assigned to former employees and by providing periodic reminders to agency security coordinators of the importance of promptly removing user access assigned to former employees. Without effective procedures to remove access, terminated employees could continue to have access to critical or sensitive resources or have opportunities to sabotage or otherwise impair entity operations or assets.

In the areas audited, the overall performance of this entity was **Good**.*

*****The rating(s) cover only audited areas and do not reflect an opinion on the overall operation of the entity. Within that context, the rating scale indicates the following:

Excellent: The audit results indicate this entity is very well managed. The report contains no findings. In addition, if applicable, prior recommendations have been implemented.

Good: The audit results indicate this entity is well managed. The report contains few findings, and the entity has indicated most or all recommendations have already been, or will be, implemented. In addition, if applicable, many of the prior recommendations have been implemented.

Fair: The audit results indicate this entity needs to improve operations in several areas. The report contains several findings, or one or more findings that require management's immediate attention, and/or the entity has indicated several recommendations will not be implemented. In addition, if applicable, several prior recommendations have not been implemented.

Poor: The audit results indicate this entity needs to significantly improve operations. The report contains numerous findings that require management's immediate attention, and/or the entity has indicated most recommendations will not be implemented. In addition, if applicable, most prior recommendations have not been implemented.

Unemployment Insurance System Data Security
Table of Contents

NICOLE GALLOWAY, CPA
Missouri State Auditor

Honorable Michael L. Parson, Governor
and
Anna S. Hui, Director
Department of Labor and Industrial Relations
Jefferson City, Missouri

We have audited certain internal controls, including security controls, designed to protect data and information maintained by the Department of Labor and Industrial Relations, Division of Employment Security, Unemployment Insurance system. This audit was conducted in fulfillment of our duties under Chapter 29, RSMo. The objectives of our audit were to:

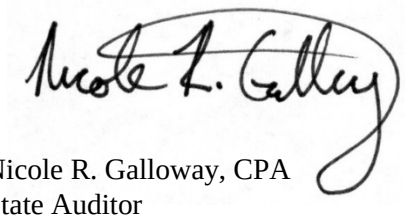
1. Evaluate the system's internal controls over significant management and financial functions, including the security and privacy controls designed to ensure the confidentiality, integrity, and availability of data and information maintained in the Unemployment Insurance system.

2. Evaluate compliance with certain legal provisions.

3. Evaluate the economy and efficiency of certain management practices and information system control activities.

We conducted our audit in accordance with the standards applicable to performance audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States. Those standards require that we plan and perform our audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides such a basis.

For the areas audited, we identified (1) deficiencies in internal controls, (2) no significant noncompliance with legal provisions, and (3) no significant deficiencies in management practices and information system control activities. The accompanying Management Advisory Report presents our finding arising from our audit of Unemployment Insurance System Data Security.



Nicole R. Galloway, CPA
State Auditor

The following auditors participated in the preparation of this report:

Director of Audits:	Jon Halwes, CPA, CGFM
Audit Manager:	Jeffrey Thelen, CPA, CISA
In-Charge Auditor:	Patrick M. Pullins, M.Acct., CISA
Audit Staff:	Kristin A. Clink, MBA

Unemployment Insurance System Data Security Introduction

Background

The Missouri Unemployment Insurance (UI) program was created by state statute to provide for the well-being of citizens. State law indicates "Economic insecurity due to unemployment is a serious menace to health, morals, and welfare of the people of this state resulting in a public calamity.[1]" The UI program is administered by the Department of Labor and Industrial Relations (DOLIR), Division of Employment Security (DES), through a federal-state partnership that was founded upon federal law but implemented through state law. In Missouri, the program is funded solely through tax contributions paid by employers, so no deductions are made from employees' paychecks for this insurance. The tax rate paid by each employer is determined by the DES, taking into account the employer's industry, claim history (how many workers have filed for UI benefits), and other adjustments allowed by state law. Taxes are due on only a portion of the wages paid to an employee (the base wage), with the base wage being subject to change based on a formula in state law.[2] In 2018, the base wage was $12,500.

Employees who lose their jobs through no fault of their own or quit for good cause related to the work or employer are eligible to file for unemployment benefits (including employees laid off from their jobs). Additionally, employees must meet certain rules regarding minimum earned wages and time frame of their employment. Employees may receive a maximum of $320 per week in benefits.

The DES utilizes a computer system known as UInteract to administer its UI responsibilities. This system, implemented in November 2016, was acquired from a vendor to replace multiple legacy computer systems that had supported the program for more than 40 years. The contractor completed the initial contract in March 2018; including providing, implementing, and trouble-shooting the system; and subsequently entered into an ongoing contract for continued maintenance of the system.

The UInteract system is web-based and accessible by claimants (employees) looking to file a claim, by employers for reporting and remitting UI taxes, and by state and private sector officials for administering the program and providing assistance to claimants searching for new jobs.

The Government Accountability Office (GAO) has included the security of information systems, including the protection of Personally Identifiable Information (PII), in the office's High-Risk List since 1997.[3] Technological

[1] Section 288.020.1, RSMo.

[2] Section 288.036.2, RSMo. The 2019 base wage decreased to $12,000.

[3] Report GAO-17-317 *Report to Congressional Committees, High Risk Series: Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others,* February 2017, is available at <http://www.gao.gov/assets/690/682765.pdf>, accessed December 4, 2018.

advances, such as lower data storage costs and increasing interconnectivity, have allowed both government and private sector agencies to collect and process extensive amounts of PII more effectively. Risks to PII can originate from unintentional and intentional threats. These risks include insider threats from careless, disgruntled, or improperly trained employees and contractors; the ease of obtaining and using hacking tools; and the emergence of more destructive attacks and data thefts.

Technology advances, combined with the increasing sophistication of individuals or groups with malicious intent, have increased the risk of PII being compromised and exposed. Correspondingly, the number of reported security incidents involving PII in both the private and public sectors has increased dramatically in recent years. At the same time, state agencies are increasingly reliant on technology and information sharing to interact with citizens and to deliver essential services. As a result, the need to protect information, including PII, against cybersecurity attacks is increasingly important.

According to accepted standards, security controls are the management, operational, and technical safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. Confidentiality refers to preserving authorized restrictions on information access and disclosure, including the means for protecting personal privacy and proprietary information. Integrity relates to guarding against improper information modification or destruction, and availability ensures timely and reliable access to and use of information. Effective privacy controls depend on the safeguards employed within the information system that is processing, storing, and transmitting PII and the environment in which the system operates. Organizations cannot have effective privacy without a basic foundation of information security. Without proper safeguards and controls, information systems and confidential data are vulnerable to individuals with malicious intentions who can use access to obtain sensitive data or disrupt operations.

The National Institute of Standards and Technology (NIST) defines cybersecurity as the process of protecting information by preventing, detecting, and responding to attacks[4] while ISACA states cybersecurity encompasses all that protects enterprises and individuals from intentional attacks, breaches, and incidents as well as the consequences.[5] Cybersecurity should be aligned with all other aspects of information security, including

[4] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1, April 2018, is available at <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf >, page 45, accessed December 4, 2018.

[5] ISACA, *Transforming Cybersecurity*, 2013, page 11.

governance, management, and assurance. The state of being secure requires maintenance and continuous improvement to meet the needs of stakeholders and the demands of emerging cyber threats.

System conversion and reporting issues

During November 2016, the state implemented a new computer system to support the operations of the DES Unemployment Insurance program. The new system, UInteract, was acquired from a contractor that modified a system previously deployed in other states to meet Missouri's requirements. DOLIR management opted to "cutover" from the legacy system to the new system, without running the two systems concurrently for a period of time in an effort to minimize the risks of data being out-of-synch between the two systems and to reduce the time necessary to complete the conversion. Approximately 2.8 billion records, were converted to the new system from the legacy system.[6]

During the UInteract design and programming phases, DOLIR management elected to custom develop reporting tools rather than utilize the vendor's optional reporting tools. However, these internally-developed reporting tools were not functional when the new system was implemented. Also, at the time of system implementation, certain control functions, such as the capability to reconcile bank account activity or to accurately determine the Maximum Benefit Amount (MBA) allowed to a claimant, were not working correctly in the new system.

During the conversion process, not all of the 2.8 billion records transferred accurately from the legacy system to the new system. DOLIR staff indicated these records were mostly older records previously entered into the legacy system's database without certain controls to ensure data was accurate and met system expectations. For example, if the legacy system accepted a value of "2" for a date in the month of February, but the new system expected "02," the record may not have been processed correctly in the new system.[7] According to DOLIR staff, the new system set these records aside until they could be modified and processed correctly.

As a result of these system implementation issues, the DES could not produce accurate Unemployment Insurance program financial and federal reports from the UInteract system for fiscal year 2017. The State Auditor's Office (SAO) fiscal year 2017 *Statewide Single Audit*[8] and *Comprehensive Annual*

[6] Records converted included several types of benefit file records, such as claims management and payments, and several types of tax file records, such as employer data and wage records.

[7] The example provided is for illustrative purposes only and does not represent the actual issues encountered in the data migration and conversion process.

[8] SAO Report No. 2018-016, *State of Missouri Single Audit, Year Ended June 30, 2017*, issued in March 2018.

Financial Report[9] audit included nine audit findings related to the Unemployment Insurance program and system implementation. Seven of the nine findings were related to system implementation, including five findings related to the new system's reporting capabilities or controls and two related to functions suspended during the conversion. The remaining two issues were for internal controls not directly related to the UInteract system conversion. DOLIR officials agreed with the substance of all findings and implemented corrective actions.

Corrective action

During fiscal year 2018, including during the process of completing the fiscal year 2017 audits, DOLIR officials took actions to remedy the issues identified by the SAO. The DOLIR submitted a Corrective Action Plan for each finding to the Missouri Office of Administration for submission to relevant oversight bodies, including the U.S. Department of Labor (DOL). In September 2018, the DOL issued a Final Determination letter to the state communicating the corrective actions taken were adequate to correct the findings identified during the fiscal year 2017 audits.

During this audit, we reviewed current processes and internal controls in place related to the UInteract system, including items such as risk assessment and security planning. We determined the underlying issues that caused the fiscal year 2017 findings have been corrected. Accordingly, we do not include any discussion of these issues in the Management Advisory Report section of this audit report.

Scope and Methodology

The scope of our audit included evaluating (1) DOLIR management's approach to and management of the UInteract system, including information security, privacy, and other relevant internal controls, (2) policies and procedures, and (3) other management functions and compliance issues in place during the period January 2016 to December 2018.

Our methodology included reviewing written policies and procedures, and interviewing various DOLIR personnel. We obtained an understanding of the applicable controls that are significant within the context of the audit objectives and assessed whether such controls have been properly designed and placed in operation. We tested certain of those controls to obtain evidence regarding the effectiveness of their design and operation. We also obtained an understanding of legal provisions that are significant within the context of the audit objectives, and we assessed the risk that illegal acts, including fraud, and violation of contract or other legal provisions could occur. Based on that risk assessment, we designed and performed procedures to provide

[9] State of Missouri, *Missouri Comprehensive Annual Financial Report For The Fiscal Year Ended June 30, 2017*, issued in January 2018, is available at <https://oa.mo.gov/sites/default/files/CAFR%202017.pdf>, accessed December 4, 2018.

reasonable assurance of detecting instances of noncompliance significant to those provisions.

We obtained data files from the UInteract system for user accounts with access to the system as of August 2018. In addition, we obtained employment records of all state employees from July 2000 to September 2018 from the statewide accounting system for human resources (SAM II). We matched these records to determine if any terminated employees had active UInteract accounts. We provided DOLIR officials a list of all terminated employees we found who had active access to the UInteract system. Although we used computer-processed data from the UInteract and SAM II systems for our audit work, we did not rely on the results of any processes performed by these systems in arriving at our conclusions. Our conclusions were based on our review of the issues specific to the audit objectives.

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

- Missouri Adaptive Enterprise Architecture (MAEA)
- National Institute of Standards and Technology (NIST)
- U. S. Government Accountability Office (GAO)
- ISACA

User Account Management

Department of Labor and Industrial Relations (DOLIR) management has not fully established controls for the maintenance of user accounts for accessing the UInteract system. Active accounts assigned to terminated users are not always removed timely. As of August 31, 2018, 1,097 accounts were assigned to users employed by the state and federal government or partner agencies, such as local job placement agencies.

The UInteract system disables a user account when the account has not been accessed for 120 days, according to DOLIR staff. In addition, system administrative functions can only be accessed from computers attached to the state's internal network. While these controls help to reduce risk, we found the UInteract system is vulnerable to the risk of unauthorized or inappropriate activity because 52 user accounts of terminated state employees were not disabled timely. This total included 2 users not employed by the DOLIR who left employment for another position in state government. These 2 users could maintain UInteract system access as long as they had continued access to the state computer network and logged in at least once every 120 days.

A terminated user is someone who has left employment and no longer needs access to the system. These 52 users had access to the UInteract system as of August 31, 2018, even though the users had terminated employment prior to August 1, 2018. DOLIR staff detected and removed the access for 44 of these users prior to auditors notifying DOLIR management of this issue.

However, the quarterly review process used by the DOLIR to detect and remove terminated user accounts did not effectively identify all accounts belonging to users not employed by the DOLIR. The remaining 8 users (including the 2 users mentioned above) whose system access had not been detected and removed by DOLIR staff were employed by other state agencies. According to the state human resources system (SAM II), these users left their jobs between April 2017 and July 2018. However, they still had active accounts as of August 31, 2018.

DOLIR management could reduce the risk of unauthorized access by increasing efforts to identify user accounts assigned to former employees and by providing periodic reminders to agency security coordinators of the importance of promptly removing user access assigned to former employees.

According to the Missouri Adaptive Enterprise Architecture (MAEA),[10] agencies must have a procedure in place for the timely notification of

[10] The Enterprise Architecture includes standards, policies, and guidelines established by Office of Administration management. The Enterprise Architecture is made up of several information technology domains, including domains dedicated to security and information. The domains define the principles needed to help ensure the appropriate level of protection for the state's information and technology assets.

administrators when a user no longer needs access. Agencies are responsible for determining which of their employees are given access to the system and for ensuring all individuals who have access still need the access. Although agencies are responsible for notifying the DOLIR to remove user access rights, DOLIR management is ultimately responsible for security of the UInteract system.

Without effective procedures to remove access, terminated employees could continue to have access to critical or sensitive resources or have opportunities to sabotage or otherwise impair entity operations or assets, according to the Government Accountability Office (GAO).

Recommendation

The DOLIR continue to improve the reviews of user accounts to ensure access of terminated or transferred employees is removed timely. In addition, the DOLIR should provide periodic reminders to other agency security coordinators of the importance of promptly requesting the removal of user access assigned to former employees.

Auditee's Response

The DOLIR agrees with the recommendation. Our planned correction actions include:

1. *Receiving a monthly list from the DOLIR Human Resources section that contains all department employees who have left employment during the month. UInteract access will be removed for individuals who are no longer employed by the DOLIR on a monthly basis.*

2. *Creating a formal UInteract System Access form that contains language reminding the requesting agency it must notify the Division of Employment Security, within 30 days, if a user no longer requires access to the UInteract system.*

3. *Sending bimonthly reminders to other agencies' security coordinators of the importance of promptly requesting the removal of user access assigned to staff who no longer require UInteract access.*