Office of Missouri State Auditor

Nicole Galloway, CPA

MissouriBUYS Statewide eProcurement System

Report No. 2018-021
April 2018

auditor.mo.gov

April 2018

Nicole Galloway, CPA
Missouri State Auditor

CITIZENS SUMMARY

Findings in the audit of the MissouriBUYS Statewide eProcurement System

User Account Management

Office of Administration (OA) management has not fully established controls for maintaining user accounts for accessing the MissouriBUYS system. The MissouriBUYS system is vulnerable to risk of unauthorized or inappropriate activity because 39 user accounts of terminated agency employees, as well as 4 unneeded user accounts of provider support personnel, were not disabled timely. The MissouriBUYS system cannot generate effective reports enabling agencies to periodically review users' access to data, to ensure access rights are commensurate with job responsibilities and remain appropriate. As a result, no such reviews have been completed. OA management does not perform supervisory reviews of system logged actions performed by privileged users or users with significant access. The OA has not documented existing security policies and procedures.

Vendor Data

A MissouriBUYS system function allows certain agency users to export vendor registration data, including limited portions of personally identifiable information (PII).

Business Contingency Planning

OA management has conceptualized MissouriBUYS system contingency plans, including major considerations and possible approaches to continue operations and to facilitate recovery of the system if necessary. However, they have not formally documented or tested the plans, including formally assigning responsibilities for oversight and maintenance of the plans.

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.

MissouriBUYS Statewide eProcurement System
Table of Contents

NICOLE GALLOWAY, CPA
Missouri State Auditor

Honorable Eric R. Greitens, Governor
and
Sarah H. Steelman, Commissioner
Office of Administration
Jefferson City, Missouri

We have audited certain internal controls, including security controls, designed to protect data and information maintained by the MissouriBUYS Statewide eProcurement 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.

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) the need for improvement in management policies and procedures. The accompanying Management Advisory Report presents our findings arising from our audit of the MissouriBUYS Statewide eProcurement system.

Nicole R. Galloway, CPA
State Auditor

The following auditors participated in the preparation of this report:

Director of Audits:	Douglas J. Porting, CPA, CFE
Audit Manager:	Jeffrey Thelen, CPA, CISA
In-Charge Auditor:	Alex R. Prenger, M.S.Acct., CPA
Audit Staff:	Kristin A. Clink, MBA

MissouriBUYS Statewide eProcurement System
Introduction

Background

The MissouriBUYS system is the state's new eProcurement system, which establishes a virtual marketplace between state departments and agencies, and vendors. Anticipated system benefits include improvements in (1) processing efficiency of requisitions, solicitations, contracts, purchase orders, invoices, and receipt of goods; (2) reporting and business intelligence; (3) identifying existing contracts and reducing spending outside of such contracts; (4) enhancing customer interaction; and (5) ensuring transparency. Examples of system features that assist these goals include a vendor registration system and public bid board. These features allow vendors to self-register and self-maintain their account, view business opportunities, and electronically submit bids or proposals. As of January 1, 2018, the system included 409 active agency users, 18,311 registered vendors, and 14,956 integrated (approved) vendors.

The state awarded the contract for the MissouriBUYS system in March 2015. Implementation efforts are still in progress. As of January 2018, major system functionality was complete, with system rollout prioritized first to central procurement personnel (purchasing and accounting) within the Office of Administration (OA), then to various power users (users with procurement duties who were ready to use the new system functionality) at select agencies. Rollout to remaining agencies is expected to conclude by July 2018. Subsequent efforts are planned to allow a degree of system participation to universities, local governments and political subdivisions.

The MissouriBUYS system replaced the state's previous On-Line Bidding and Vendor Registration system. Additionally, once rollout to the remaining agencies concludes, the Statewide Advantage for Missouri (SAM II) Financial system's procurement capabilities will be disabled, and agency-specific procurement systems and websites phased out.

The MissouriBUYS system is provided by Perfect Commerce (PC), managed by the OA, and structured under the Software as a Service (SaaS) model of cloud computing. The National Institute of Standards and Technology (NIST) defines the SaaS model as the capability provided to the consumer to use the provider's applications running on a cloud infrastructure (the underlying collection of hardware and software not managed or controlled by the consumer).[1] The SaaS model approach divides ongoing responsibilities between the PC and OA.

As the system provider, PC is responsible for ensuring the underlying cloud infrastructure operates sufficiently to support the system, programming

[1] National Institute of Standards and Technology, SP 800-145 The NIST Definition of Cloud Computing, September 2011, is available at <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>.

system changes and releasing updates to the OA for approval, performing database and security administration, and planning for disaster recovery (the technical actions needed to restore MissouriBUYS after a disaster).

As the system manager, the OA is responsible for ensuring contractual requirements are met; testing and approving updates developed by PC; maintaining policies and procedures for use of the system; processing security requests to add, change, or remove user access; and planning for business contingencies (the decisions needed to continue business operations affected by MissouriBUYS unavailability, which may invoke disaster recovery plans). The OA Division of Accounting is directly and predominantly involved in all of these tasks, but is assisted by the OA Division of Purchasing and the OA Information Technology Services Division (ITSD) to varying degrees and circumstances. Additionally, as the system data owner, the OA is ultimately accountable for system and information confidentiality, integrity and availability.

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 personally identifiable information (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.

Scope and Methodology

The scope of our audit included internal controls established and managed by the OA, policies and procedures, and other management functions and compliance issues in place during the period July 2017 to January 2018. Our scope did not include internal controls that are the responsibility of agencies using the MissouriBUYS system.

Our methodology included reviewing written policies and procedures, interviewing various OA personnel, and performing testing. 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 reasonable assurance of detecting instances of noncompliance significant to those provisions.

We obtained data files from the MissouriBUYS system of user accounts having access to the system as of September 2017. Additionally, we obtained employment records of all state employees from the SAM II system. We matched these records to determine if any terminated employees had active MissouriBUYS user accounts. We provided OA officials lists of all terminated employees we found who had active access to the MissouriBUYS system, and unneeded provider support accounts.

Although we used computer-processed data from the MissouriBUYS 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 controls from the following sources:

- Missouri Adaptive Enterprise Architecture (MAEA)
- National Institute of Standards and Technology (NIST)
- Government Accountability Office (GAO)
- ISACA (previously known as the Information Systems Audit and Control Association)

1. User Account Management

Office of Administration (OA) management has not fully established controls for maintaining user accounts for accessing the MissouriBUYS system. Accounts assigned to terminated agency users are not always removed timely, and system provider support personnel accounts were not removed once no longer required. In addition, the system cannot generate effective reports to enable periodic reviews of user access rights; periodic supervisory reviews of privileged user actions are not performed; and existing procedures are not documented.

1.1 Termination of user accounts

The MissouriBUYS system is vulnerable to the risk of unauthorized or inappropriate activity because 39 user accounts of terminated agency employees, as well as 4 unneeded user accounts of provider support personnel, were not disabled timely.

OA management has established procedures to detect and remove such accounts. However, prior to our review of user accounts, they had only completed sporadic reviews. According to OA management, system implementation efforts have been prioritized to ensure major system functionalities were achieved. While implementation efforts were critical to the system's success, this prioritization reduced the consistency and effectiveness of established controls because terminated agency employees and some unnecessary provider support personnel continued to have active MissouriBUYS system access.

Terminated agency users

At the time of our review, 39 former employees of several state agencies still had access to the system 30 days or more after terminating employment from the agency that had granted the user access. Three of these users still had access to the system for more than a year before being removed.

OA 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),[2] agencies must have a procedure in place for the timely notification of administrators when a user no longer needs access. MissouriBUYS procedures place the responsibility for identification of accounts belonging to terminated and transferred users with the agency employing the users. Agencies are responsible for determining which of their employees are given

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

access to the system and for ensuring all individuals who have access still need the access. When an agency user no longer needs access, MissouriBUYS procedures require agency security coordinators to submit a form to the OA security administrator requesting removal of the user's access to the system.

Although agencies are responsible for submitting requests to add, change, or remove user access rights, OA management is ultimately responsible for security of the system.

Provider accounts no longer required

At the time of our review, 4 user accounts assigned to system provider support personnel were not removed when access was no longer required. Of these, 3 were generic accounts used by specific provider support personnel before more formal, individualized accounts were established. OA personnel detected these three accounts and required the provider use individualized accounts, but did not follow through to ensure the accounts had been timely disabled. These accounts were disabled when we discussed this issue with OA management.

According to accepted standards, organizations should remove, disable or otherwise secure unnecessary accounts. Only OA management can authorize and subsequently have provider accounts removed; agencies have no responsibility for such accounts.

Conclusion

Effective procedures are especially important because the system's web-based nature allows agency employees and provider support personnel access from their homes, mobile devices, and other locations until their account is removed.

Without effective procedures to remove access, terminated employees and provider accounts that are no longer required 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).

1.2 Review of user access

The MissouriBUYS system cannot generate effective reports enabling agencies to periodically review users' access to data, to ensure access rights are commensurate with job responsibilities and remain appropriate. As a result, no such reviews have been completed.

As users' work assignments and job responsibilities change, access rights to the MissouriBUYS system may be added, changed, or removed. Over time, users can accumulate access rights that are no longer necessary, increasing the risk of inappropriate access to system data. According to the MAEA, agencies must periodically review user accounts for levels of authorized access for each user. However, agencies rely on OA management to provide system reports enabling such reviews. OA management told us they are working to create more detailed reports of users' security access.

Without periodically reviewing user access rights, there is an increased risk that unauthorized alterations of the rights will go undetected or that access rights may not be aligned with current job duties.

1.3 Privileged user supervision

OA management does not perform supervisory reviews of system logged actions performed by privileged users or users with significant access.

Privileged users, including OA administrative personnel and limited provider support personnel, have extensive access rights needed to keep the system and associated procedures running efficiently. The actions of privileged users warrant supervision due to the extensive rights these users are provided. However, OA management did not provide supervisory oversight or establish other mitigating controls to ensure these privileged users performed only authorized functions. Changes made by privileged users or users with significant access to MissouriBUYS are logged, but logs are not reviewed regularly for this purpose. According to OA management, supervisory reviews are not currently performed because the privileged users or users with significant access are individuals who work with OA management daily towards crucial system implementation efforts.

Routinely monitoring privileged user actions can help identify significant problems and deter individuals from inappropriate activities. Without effective monitoring, an increased risk exists that these individuals could perform unauthorized system activities without being detected.

1.4 Documentation of security policies and procedures

The OA has not documented existing security policies and procedures, including those to:

- Request, establish and maintain system accounts.
- Timely notify security administrators of employee transfers and terminations.
- Close user accounts and remove access rights for transferred or terminated employees once security administrators are notified.
- Describe assignment and use of privileged system level accounts.

We confirmed the existence of these informal policies and procedures through discussions held with OA management. However, at least some of the existing policies and procedures were not documented because OA management prioritized system implementation efforts, as discussed in MAR finding number 1.1.

According to accepted standards, documentation of all aspects of computer support and operations is important to ensure continuity and consistency. Formalizing operational practices and procedures with sufficient detail helps to eliminate security lapses and oversights, gives new personnel sufficiently detailed instructions, and provides a quality assurance function to help ensure that operations will be performed correctly and efficiently.

Without documented and approved policies and procedures, management may not have assurance that control activities are appropriate and properly applied.

Recommendations

The OA:

1.1 Periodically review user accounts to ensure access of terminated or transferred employees, as well as provider support accounts that are no longer required, is removed timely. In addition, ensure frequent reminders are provided to agency security coordinators of the importance of promptly removing user access assigned to former employees.

1.2 Work with the provider to ensure MissouriBUYS is capable of generating effective reports to assist agencies with reviews of user access.

1.3 Perform periodic supervisory reviews of defined actions performed by privileged users or users with significant access.

1.4 Fully document and periodically review security policies and procedures.

Auditee's Response

1.1 The OA will provide employee access reports to all agencies on a monthly basis. Additionally, the OA has already implemented an improved policy of immediately "inactivating" users in MissouriBUYS once the individual has been terminated in Statewide Advantage for Missouri (SAM II) Financial or SAM II Human Resources. This will remove the ability for activity to occur.

1.2 We concur. We are working on improved reporting capabilities.

1.3 We concur. We are conducting additional supervisor reviews of system activity.

1.4 We concur. We are improving system documentation.

2. Vendor Data

A MissouriBUYS system function allows certain agency users to export vendor registration data, including limited portions of personally identifiable information (PII). While export capabilities are common in information systems to fulfill legitimate functions, controls could be strengthened by restricting these capabilities to only those individuals who need such access to perform job functions.

OA management said they spoke to the system provider about establishing export restrictions and determined this capability could be developed and implemented. However, OA management has not formally requested the provider to implement export restrictions.

According to the GAO, PII refers to any information about an individual maintained by an entity, including any information that can be used to distinguish or trace an individual's identity, and any other information which is linked or linkable to an individual. According to ISACA, entities should secure information assets, potentially by restricting use and distribution of information. Otherwise, there is an increased risk that vendor data and PII will be inappropriately used or inadvertently disclosed.

Recommendation

The OA work with the provider to increase restrictions to the system's function to export vendor data, including PII.

Auditee's Response

The OA already has significant controls including mandatory background checks, employee acknowledgement of appropriate conduct, and a limited number of departmental employees authorized to request access to the MissouriBUYS system. The OA agrees to discuss the strengthening of security controls with the vendor; however, the current controls are strong.

Auditor's Comment

While we acknowledge the OA has certain critical controls in place, more can be done to strengthen security and protect information, as the OA agreed with. Limiting the ability to export vendor data to only those users who need such access to perform their jobs provides an additional layer of security, effectively helping to minimize risk of misuse of PII.

3. Business Contingency Planning

OA management has conceptualized MissouriBUYS system contingency plans, including major considerations and possible approaches to continue operations and to facilitate recovery of the system if necessary. However, they have not formally documented or tested the plans, including formally assigning responsibilities for oversight and maintenance of the plans.

Contingency planning provides an efficient approach for the timely recovery and restoration of critical processes, including business operations, according to the MAEA. Contingency plans establish policies, procedures, and technical measures that can enable operations, systems, and data to be recovered quickly and effectively following a service disruption or disaster. According to accepted standards, contingency plans should be reviewed for accuracy and completeness at least annually or whenever significant changes occur to any element of the plan.

While responsibility for maintaining the contingency plan has been informally assigned, OA management has not documented the formal assignment of specific responsibilities for maintaining the contingency plans. According to OA management, plans have not been documented and responsibilities have not been formally assigned due to business contingency similarities between the MissouriBUYS and SAM II systems, including personnel who would carry out the plans. However, plans for the MissouriBUYS system require unique considerations over the SAM II system due to its SaaS structure.

Without a formally documented or tested contingency plan, management has limited assurance the organization's business functions can be sustained during or promptly resumed after a disruptive incident. Without a formal designation of staff responsible for oversight and maintenance, there is increased risk that contingency plans and related policies and procedures may not remain current, potentially impacting the ability to promptly restore the system and related business functions.

Recommendation

The OA should either add MissouriBUYS considerations to its existing SAM II contingency plan, or formally create a standalone MissouriBUYS contingency plan, and formally assign responsibilities for development, implementation, and maintenance of the plan to appropriate personnel. Once established, the plan should be tested on a periodic basis.

Auditee's Response

The OA will add MissouriBUYS to its existing SAM II contingency plan.