Nicole Galloway, CPA

Missouri State Auditor

Missouri WIC Information Network System
Data Security

Report No. 2021-049

August 2021

auditor.mo.gov

Findings in the audit of Missouri WIC Information Network System Data Security

User Account Management	The Missouri WIC Information Network System (MOWINS) is vulnerable to the risk of unauthorized transactions being processed, and records being improperly viewed, because user accounts of terminated users at local agencies, such as county health departments, are not always removed timely.
Design of User Roles	Department of Health and Senior Services (DHSS) management has not adequately designed user roles in the MOWINS to segregate incompatible job functions.
Service Level Agreement	The DHSS and the Office of Administration (OA) - Information Technology Services Division (ITSD) do not have a comprehensive or up-to-date service level agreement for information technology (IT) services provided by the ITSD to the DHSS.
Documentation of Security Controls	The DHSS has not documented policies and procedures for certain security controls of the MOWINS.

> 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.

All reports are available on our Web site: auditor.mo.gov

Missouri WIC Information Network System Data Security
Table of Contents

NICOLE GALLOWAY, CPA
Missouri State Auditor

Honorable Michael L. Parson, Governor
      and
Robert J. Knodell, Acting Director
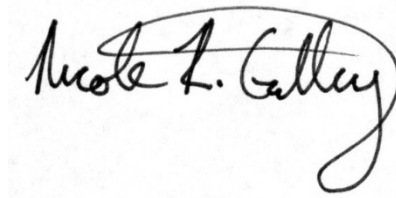Department of Health and Senior Services
Jefferson City, Missouri

We have audited certain internal controls, including security controls, designed to protect data and information maintained by the Department of Health and Senior Services, Missouri WIC Information Network System (MOWINS). 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.

4. Evaluate the effectiveness of information security controls for protecting the confidentiality, integrity, and availability of significant systems and information.

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, (3) the need for improvement in management practices and information system control activities, and (4) the need for improvement in information security controls.

The accompanying Management Advisory Report presents our findings arising from our audit of Missouri WIC Information Network 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: Alex R. Prenger, M.S.Acct., CPA, CISA, CFE, CGAP
In-Charge Auditor: Patrick M. Pullins, M.Acct., CISA, CFE
Audit Staff: Zachery L. Harris

Missouri WIC Information Network System Data Security

Introduction

Background

The Special Supplemental Nutrition Program for Women, Infants, and Children - better known as the WIC Program - serves to safeguard the health of low-income pregnant, postpartum, and breastfeeding women, infants, and children up to age 5 who are at nutritional risk by providing nutritious foods to supplement diets, information on healthy eating including breastfeeding promotion and support, and referrals to health care.

To participate in the program, household income may be no more than 185% of the federal poverty income guidelines ($49,025 for a household of four persons as of April 1, 2021). Families that qualify for the supplemental nutrition assistance program (SNAP) or temporary assistance for needy families (TANF) program automatically qualify. Individuals who meet income and category guidelines will have a nutrition and health assessment during the certification process.

The WIC program is administered at the federal level by the Food and Nutrition Service of the U.S. Department of Agriculture. In Missouri, it is administered by the Department of Health and Senior Services (DHSS), Division of Community and Public Health, Section for Healthy Families and Youth, Bureau of WIC and Nutrition Services. The bureau uses a software program called the Missouri WIC Information Network System (MOWINS) to administer the program. The system is maintained by the Office of Administration (OA) - Information Technology Services Division (ITSD) in conjunction with the vendor.

MOWINS is an implementation of SPIRIT software (Successful Partners in Reaching Innovative Technology), which was developed and is used by a consortium of 23 states, territories, and Indian tribal organizations. The SPIRIT system is currently being redeveloped into a web-based system, referred to as SPIRITweb, with planned implementation by partner states to begin in July 2022. It is unknown when Missouri will implement the new software. Missouri currently serves as the lead state for this redevelopment project and has primary responsibility for monitoring the efforts of the contracted partner. Members of the consortium belong to various boards and committees charged with overseeing certain aspects of the SPIRIT system on behalf of the consortium, including the SPIRIT User Group, the Change Control Work Group, the Executive Steering Committee, and the Technology Advisory Group. Each member of the consortium implements its own instance of the SPIRIT system and maintains its own data repositories for participants.

As of December 2020, Missouri had 92,272 participants in the WIC program as follows:

Figure 1: Missouri WIC Participants, December 2020
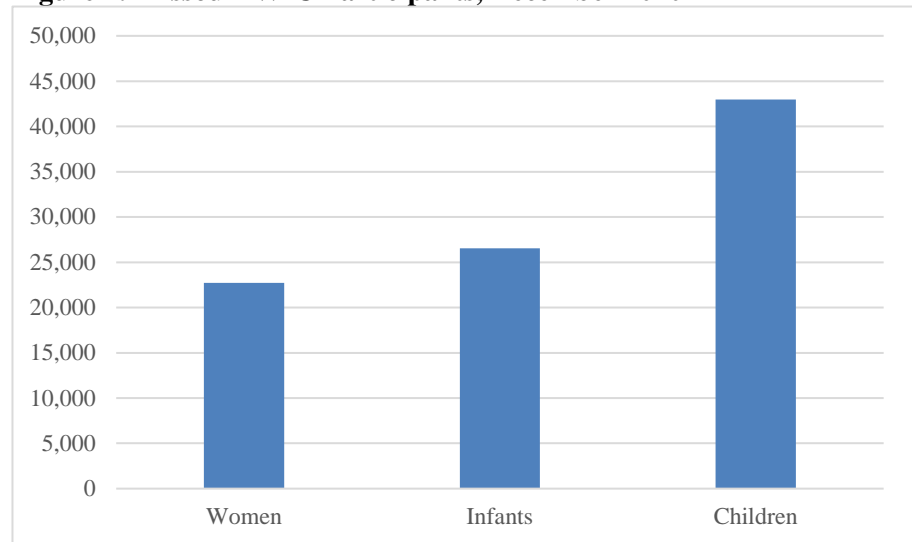
Source: National Data Bank, U.S. Department of Agriculture, Food and Nutrition Service

The Government Accountability Office (GAO) has included the security of information systems in the office's High-Risk List since 1997, specifically adding the protection of Personally Identifiable Information (PII) in its 2015 update.[1] Technological 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

---

[1] Report GAO-19-157SP, *Report to Congressional Committees, High Risk Series: Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas,* March 2019, is available at <https://www.gao.gov/assets/gao-19-157sp.pdf>, accessed June 15, 2021.

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[2] while ISACA states cybersecurity encompasses all that protects enterprises and individuals from intentional attacks, breaches, and incidents as well as the consequences.[3] Cybersecurity should be aligned with all other aspects of information security, including 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.

Scope and Methodology

The scope of our audit included evaluating (1) DHSS management's approach to and management of the MOWINS, 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 year ended December 31, 2020.

Our methodology included reviewing written policies and procedures, interviewing various DHSS and ITSD personnel, and performing testing. We obtained an understanding of internal control that is significant to the audit objectives and planned and performed audit procedures to assess internal control to the extend necessary to address the audit objectives. We also

---

[2] 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 June 15, 2021.

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

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.

Authorized users of the MOWINS include state users (DHSS employees) and local agency users (employees from entities such as county health departments).

We reviewed authorized users to determine if any terminated employees had active user accounts. For state users, we obtained employment records of all state employees from the statewide accounting system, Statewide Advantage for Missouri (SAM II), and matched these records against all state users. We did not identify any terminated state users. For local users, we judgmentally selected a sample of 9 local agencies, and contacted officials at each agency to confirm the appropriateness of the active user accounts. We based our sample selection on several factors, including geographic distribution, count of registered users, and type of entity (hospital-based or county-based, combined city/county, single county, or multiple county). In addition, we selected counties with ongoing State Auditor's Office audits. Because we judgmentally selected our test items, our results cannot be projected to the populations of 118 entities or 765 local agency users.

We also reviewed authorized users to determine if assigned access rights were excessive or resulted in incompatible functions. For certain state users, we discussed with DHSS officials those users' job responsibilities, in comparison to their assigned rights. For all 765 local agency users (including roles assigned at multiple entities, in the cases of local users who worked for more than one entity), we reviewed system documentation provided by the DHSS identifying the roles that could and could not be assigned to users with different job functions.

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

1. User Account Management

The Missouri WIC Information Network System (MOWINS) is vulnerable to the risk of unauthorized transactions being processed, and records being improperly viewed, because user accounts of terminated users at local agencies, such as county health departments, are not always removed timely. A terminated user is someone who has left employment with an entity and no longer needs access to the system. We found, for a selection of 96 local agency user accounts tested, 5 former employees who still had access to the system.

Currently, the Department of Health and Senior Services (DHSS) does not formally review user accounts for inappropriate access, except during on-site visits every 2 years. Instead, that responsibility is assigned to local agency security coordinators. Each agency accessing the MOWINS must appoint a security coordinator who is responsible for approving user requests to access the system. The coordinators are also responsible for periodically (at least twice a year) reviewing users at their agencies to identify any users no longer needing access. DHSS policy requires coordinators to submit a request to the DHSS to add or remove the applicable user account(s) when a change is needed.

DHSS 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),[4] entities must have a procedure in place for the timely notification of administrators when a user no longer needs access. In addition, entities are responsible for determining who is given access to the system and for ensuring all individuals who have access still need the access. When a user no longer needs access, the entity should submit a form to the security administrator requesting removal of the user's access to the 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 DHSS more frequently review local agency user accounts to ensure access of terminated or transferred employees is removed, and provide more

---

[4] 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.

frequent reminders to local agency security coordinators of the importance of promptly removing user access assigned to former employees.

Auditee's Response

DHSS concurs with this recommendation. The department currently has processes in place for monitoring staff access but will update policies and procedures to include specific guidance. Any user that has not accessed MOWINS in the last 30 days will have their user ID access updated to inactive. The MOWINS Help Desk staff will also send out a monthly email message requesting all local agency staff to review the employees who have access to their agency site. The email message will also include instructions on how to report a user who is no longer employed or transferred to another agency. DHSS will also update WIC policy to instruct immediate notification to DHSS for employees that have left or transferred, and to include violations that can be given should it be discovered that the DHSS was not notified within 30 days. Changes for monitoring will occur immediately, while updates to WIC policies will not be finalized until October 2022.

2. Design of User Roles

DHSS management has not adequately designed user roles in the MOWINS to segregate incompatible job functions. Certain roles are poorly defined, allowing some users with those roles access to the system that is inappropriate for their position, and one role unnecessarily allows access to all local agency functions of the system.

The MOWINS uses security roles to define access to the system. Users are assigned to an individual role or roles. These roles each allow access to a subset of system functions. Roles are generally designed according to the user's job functions. For example, a clerk may have access to schedule appointments and view clinic notes, but not to approve a participant's claim for benefits. If users have multiple roles concerning the same system information, the role with the most access prevails for all roles assigned in the event of a conflict. For example, if two separate roles respectively allow view-only and edit access to the same information, a user with both roles assigned can edit the information. In addition, users' access is limited by the specific agencies and sites the user is set up to access. Users can be assigned to multiple combinations of roles, agencies, and sites.

Local agency user roles

One role is assigned to both staff and supervisors fulfilling certain clinical functions at local agencies who assist participants in applying for Special Supplemental Nutrition Program for Women, Infants, and Children (WIC) benefits. System documentation specifies that staff assigned to this role should not also be given concurrent access to other conflicting system roles that require a higher level of user education and certification. Any staff assigned to this role and also to a conflicting role has inappropriate access. Supervisors, however, are permitted concurrent access. We determined 15 users held a combination of this role and one or more conflicting roles.

An additional situation exists in a second role that is assigned to both staff and supervisors of local agencies. In this instance, the shared role allows access to almost all local agency functions of the system. Supervisors are allowed to have this role, but staff are not. We identified 217 local users assigned to this role.

Information to determine whether users with these two roles were staff or supervisors was not readily available. We provided DHSS management a list of the users for further review and potential action. The DHSS could also better define, prevent, and detect potential conflicts and inappropriate access by creating separate roles for the staff and supervisor positions.

State user role

A similar situation involves state users assigned a third role that has excessive access to system administration functions. DHSS officials indicated the users need access to certain administrative functions to perform their job responsibilities. However, this third role also enables access to other administrative functions not necessary for these users' responsibilities. Creating a separate role for these users would prevent this unnecessary access.

Conclusion

By reviewing the levels of system access assigned to roles and creating new roles with access rights better aligned to job responsibilities as appropriate, the DHSS can better control the access given to system users and help prevent inappropriate access from being granted in the system. This change would increase system security by reducing the risk of a user, accidentally or maliciously, making inappropriate changes to the system or its data.

Recommendation

The DHSS review the design of system roles and make changes necessary to appropriately limit access to the system and segregate incompatible functions. In addition, the DHSS should review the provided list of current local users for appropriateness and potential action.

Auditee's Response

DHSS concurs with this recommendation. The department will review all current roles, the permissions assigned to that role, and make appropriate changes to limit access by removing permissions or by creating roles to limit access. After review and updates to the roles are made, the department will review all MOWINS access and update accordingly for each user ID. DHSS will review and implement any new changes by October 2022. Any minor corrections that can be made immediately will be executed prior to October 2022.

3. Service Level Agreement

The DHSS and the Office of Administration (OA) - Information Technology Services Division (ITSD) do not have a comprehensive or up-to-date service level agreement for information technology (IT) services provided by the ITSD to the DHSS. As a result, the responsibilities and expectations between both parties are not fully established or documented.

A service level agreement (SLA) is a document used by organizations entering into a partnership for the provision of IT services. According to ISACA, a SLA is used to align IT enabled products and services and service levels with enterprise needs and expectations, including identification, specification, design, publishing, agreement, and monitoring of IT products and services. SLAs can be in-house between an organizational unit and its IT department, external between an entity and an outside service provider, or internal within the units of a service provider.[5]

An SLA is crucial to promote continuous and open communication between the parties to the agreement. Without such communication, there is an increased risk the customer and the service provider will not appropriately understand or respond to each other's expectations. This weakness could result in confusion or frustration, or potentially more severe outcomes such as system failure or data loss.

According to the *Information Systems Control Journal*,[6] a "SLA is a necessity between a service provider and service beneficiary because a service can be called 'bad' or 'good' only if this service is clearly described. Moreover, it formalizes the needs and expectations of the organization and serves as a kind of guarantee for both parties. In this way, potential misunderstandings are reduced and a clear view is given on the priorities of the service and its delivery. . . . A balanced SLA is a compromise between the needs, expectations and requirements of the organization (user group) and the service provision capabilities and promises of the service provider. At the same time, it must protect the service provider by limiting liability, identifying responsibilities and rationally managing user expectations."

Recommendation

The DHSS work with the ITSD to develop a new service level agreement that specifies services to be provided and addresses communications between the agencies.

Auditee's Response

DHSS concurs with this recommendation. The department will work closely with ITSD to develop and implement a new Service Level Agreement (SLA) that will be reviewed and updated on a yearly basis. DHSS will begin working with ITSD to have a new SLA in place by October 2022.

4. Documentation of Security Controls

The department has not documented policies and procedures for certain security controls of the MOWINS.

---

[5] Van Grembergen, Wim, Ph.D., Steven De Haes and Isabelle Amelinckx. "Using COBIT and the Balanced Scorecard as Instruments for Service Level Management." *Information Systems Control Journal*, Volume 4 (2003): 56-62.

[6] Ibid.

According to the GAO's standards for internal control, control activities are an integral part of an organization's planning, implementing, reviewing, and accountability for stewardship of government resources and achieving effective results. Control activities are the policies, procedures, techniques, and mechanisms that enforce management's directives and help ensure that actions are taken to reasonably address risks. The following control activities have not been fully documented:

- Policies and procedures related to system backups, recovery, and backup retention.

- Documentation to support the completion of security training by state staff accessing the system.

- Procedures for handling lost or compromised user IDs and passwords.

- Specifications documenting what security-related events are logged, and how those logs are managed, retained, and destroyed when no longer useful.

- Policies identifying and stating the responsibilities of system and data owners.

- Procedures and documentation to support certain reviews of local agencies by state Technical Assistance staff, held every 2 years.

DHSS staff indicated that much of this information is communicated to users by on-the-job training and other informal processes.

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 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.

Recommendation

The DHSS fully document and regularly review documentation of key security controls.

Auditee's Response

DHSS concurs with these recommendations. The department will provide procedures for related control activities referenced in this audit by updating policies, creating new procedures, and educating all staff who are impacted.

The department will incorporate language into the SLA when applicable. After approval of new procedures, applicable information will be shared with local and state agency staff to provide better support. DHSS will have updates in place by October 2022. Any communication or minor corrections that can be made immediately will be executed prior to October 2022.