LA22-12

STATE OF NEVADA

Performance Audit

Department of Health and Human Services
Division of Health Care Financing and Policy

Information Security

2021

Legislative Auditor
Carson City, Nevada

Audit Highlights

Highlights of performance audit report on the Division of Health Care Financing and Policy, Information Security issued on March 22, 2022.

Legislative Auditor report # LA22-12.

Background

The mission of the Division of Health Care Financing and Policy (Division) is to: 1) purchase and provide quality health care services to low-income Nevadans in the most efficient manner, 2) promote equal access to health care at an affordable cost to the taxpayers of Nevada, 3) restrain the growth of health care costs, and 4) review Medicaid and other state health care programs to maximize potential federal revenue. The Division administers both Nevada Medicaid and Check Up programs.

The Medicaid Management Information System (MMIS) is a computerized claims processing and information retrieval system the Nevada Medicaid program must have to be eligible for federal funding.

In fiscal year 2021, the Division was primarily funded with federal grants totaling $3.7 billion and state appropriations of about $873 million. As of June 2021, the Division had 261 filled positions located in its Carson City, Elko, Las Vegas, and Reno offices. Eighteen of these positions are dedicated to information technology (IT) activities. One position leads the Business Process Management Unit; three support the Information Security Office; six support the Project Management Office; and eight provide support for the Division's systems, network, and help desk.

Purpose of Audit

The purpose of the audit was to determine if the Division of Health Care Financing and Policy has adequate controls to ensure user access controls protect its sensitive information and to monitor its MMIS change management process. The audit included the systems and practices in place during fiscal year 2021, and fiscal year 2020 for enhancement projects.

Audit Recommendations

This audit report includes six recommendations to improve information security access controls to users of the Medicaid Management Information System.

The Division accepted the six recommendations.

Recommendation Status

The Division's 60-day plan for corrective action is due on June 15, 2022. In addition, the 6-month report on the status of audit recommendations is due on December 15, 2022.

For more information about this or other Legislative Auditor reports go to: http://www.leg.state.nv.us/audit (775) 684-6815.

Information Security

Division of Health Care Financing and Policy

Summary

The background investigation process at the Division can be strengthened. Specifically, non-Division state employees and Division IT contractors were given access to the Medicaid Management Information System without verifying or documenting a background check was completed. In addition, some fiscal agent employees' user accounts were enabled before the Division received background investigation information and authorized access. Finally, newly hired Division employees did not receive a preliminary background investigation or submit their background investigation packet before they were given access to MMIS. Background investigations help reduce the risk sensitive data will be accessed by disreputable individuals.

The Division does not actively manage MMIS user accounts. Specifically, the Division does not ensure MMIS access is still needed for non-Division state employees. In addition, the Division does not ensure that user accounts of former state employees and its fiscal agent are disabled timely. Finally, the Division does not ensure documentation used to authorize user MMIS access is complete or reviewed periodically. Accounts still valid after a user leaves an enterprise make it easier for an external or internal threat actor to gain unauthorized access to enterprise data using valid user credentials.

Key Findings

The Division did not verify or document background investigations were performed for non-Division state employees and Division IT contractors that were granted access to MMIS. For 84 non-Division employees, the Division did not verify background checks were performed. In addition, we randomly selected 7 of the Division's 13 IT contractors for testing. For four of seven (57%) contractors tested, the Division had no record a background investigation was conducted. (page 3)

Fiscal agent staff were given MMIS access before proper authorization. We identified 2 of 10 (20%) fiscal agent user accounts that were enabled in the system prior to the background investigation process being initiated and authorized by the Division. (page 4)

For all newly hired Division employees in fiscal year 2021, access was granted to MMIS prior to completing a preliminary or fingerprint background investigation. A preliminary background investigation consists of a national records check that provides detailed background information based on someone's name and Social Security number and can be performed before a more thorough fingerprint background check. (page 5)

The Division does not have a process to actively manage non-Division state employee user accounts and ensure system access is still needed. For 11 of 79 (14%) non-Division state employee MMIS user accounts tested, the employee had never logged into MMIS since being given access. Three accounts have remained enabled for over 2 years without any login activity. In addition, nine other employees have not logged into MMIS since before June 2021. One employee has not logged into the system for over 2.5 years. Instead of actively managing user accounts, the Division relies on other state agencies and the fiscal agent to notify them when access is no longer needed. (page 7)

During our testing of user accounts, we identified four non-Division state employees that ended state employment before June 30, 2021, while their user accounts remained active for months after they terminated employment with the State. In addition to state employees, we tested accounts of all seven fiscal agent users who were identified as terminated. One account was disabled the same day of termination while six remained enabled for several days to several months. (page 7)

The Division did not properly document system access authorization or documentation was inaccurate on the MMIS security access request forms. For 23 non-fiscal agent system access forms tested, we observed for some forms supervisor or information security officer approval was not documented, user roles were not documented, or approved user roles did not agree to user roles assigned in the system. In addition, the Division could not provide system access request forms for three users. (page 9)

The Division's MMIS enhancement process is effective in ensuring changes to the system are prioritized and completed. A documented change management plan is utilized and monitored. In addition, the Division monitors hours charged to individual projects. Proper management of this process helps ensure changes to the MMIS meet the needs of stakeholders and align with available resources. (page 11)

Audit Division
Legislative Counsel Bureau

STATE OF NEVADA

LEGISLATIVE COUNSEL BUREAU

CARSON CITY OFFICE
LEGISLATIVE BUILDING
401 S. CARSON STREET
CARSON CITY, NEVADA 89701
(775) 684-6800

LAS VEGAS OFFICE
GRANT SAWYER STATE OFFICE BUILDING
555 E. WASHINGTON AVENUE, SUITE 4400
LAS VEGAS, NEVADA 89101
(702) 486-2800

Legislative Commission
Legislative Building
Carson City, Nevada

This report contains the findings, conclusions, and recommendations from our performance audit of the Department of Health and Human Services, Division of Health Care Financing and Policy, Information Security. This audit was conducted pursuant to the ongoing program of the Legislative Auditor as authorized by the Legislative Commission. The purpose of legislative audits is to improve state government by providing the Legislature, state officials, and Nevada citizens with independent and reliable information about the operations of state agencies, programs, activities, and functions.

This report includes six recommendations to improve information security access controls to users of the Division's Medicaid Management Information System. We are available to discuss these recommendations or any other items in the report with any legislative committees, individual legislators, or other state officials.

Respectfully submitted,

Daniel Crossman

Daniel L. Crossman, CPA
Legislative Auditor

March 7, 2022
Carson City, Nevada

Division of Health Care Financing and Policy Information Security

Table of Contents

Introduction

Background

The mission of the Division of Health Care Financing and Policy (Division) is to: 1) purchase and provide quality health care services to low-income Nevadans in the most efficient manner, 2) promote equal access to health care at an affordable cost to the taxpayers of Nevada, 3) restrain the growth of health care costs, and 4) review Medicaid and other state health care programs to maximize potential federal revenue. The Division works in partnership with the Centers for Medicare and Medicaid Services (CMS) to assist in providing quality medical care for eligible individuals and families.

The Division administers both Nevada Medicaid and Check Up programs. Medicaid provides health care coverage for many people including low-income families with children whose family income is at or below 133% of the Federal Poverty Level (FPL); Supplemental Social Security Income recipients; certain Medicare beneficiaries; and recipients of adoption assistance, foster care, and some children aging out of foster care. Check Up provides health care benefits to uninsured children from low-income families who are not eligible for Medicaid, but whose family income is at or below 200% of the FPL. The Division of Welfare and Supportive Services determines eligibility for Nevada Medicaid and Check Up programs.

The Medicaid Management Information System (MMIS) is a computerized claims processing and information retrieval system the Nevada Medicaid program must have to be eligible for federal funding. The MMIS includes automated claims processing and subsystems that support program integrity activities such as: provider screening, claim processing, and utilization reviews. CMS validates and certifies states' MMIS systems.

Once certified, states may receive 75% federal financial participation for the operation of this system. The Nevada MMIS is implemented, managed, and maintained by a contractor known as a fiscal agent. In fiscal year 2021, expenditures to the fiscal agent totaled over $37 million.

In fiscal year 2021, the Division was primarily funded with federal grants totaling $3.7 billion and state appropriations of about $873 million. As of June 2021, the Division had 261 filled positions located in its Carson City, Elko, Las Vegas, and Reno offices. Eighteen of these positions are dedicated to information technology activities. One position leads the Business Process Management Unit; three support the Information Security Office; six support the Project Management Office; and eight provide support for the Division's systems, network, and help desk.

Scope and Objective

The scope of our audit covered the systems and practices in place during fiscal year 2021, and fiscal year 2020 for enhancement projects. Our audit objective was to:

- Determine if the Division of Health Care Financing and Policy has adequate controls to ensure user access controls protect its sensitive information and to monitor its MMIS change management process.

This audit is part of the ongoing program of the Legislative Auditor as authorized by the Legislative Commission and was made pursuant to the provisions of Nevada Revised Statutes 218G.010 to 218G.350. The Legislative Auditor conducts audits as part of the Legislature's oversight responsibility for public programs. The purpose of legislative audits is to improve state government by providing the Legislature, state officials, and Nevada citizens with independent and reliable information about the operations of state agencies, programs, activities, and functions.

Background Investigation Process Can Be Strengthened

The background investigation process at the Division of Health Care Financing and Policy (Division) can be strengthened. Specifically, non-Division state employees and Division information technology (IT) contractors were given access to the Medicaid Management Information System (MMIS) without verifying or documenting a background check was completed. In addition, some fiscal agent employees' user accounts were enabled before the Division received background investigation information and authorized access. Finally, newly hired Division employees did not receive a preliminary background investigation or submit their background investigation packet before they were given access to MMIS. Background investigations help reduce the risk sensitive data will be accessed by disreputable individuals.

The MMIS contains protected health information which includes any information about health status, provision of health care, or payment for health care. In addition, MMIS processes the electronic record of health-related information on patients that can be created, gathered, managed, and consulted by authorized individuals. As of July 2021, there were 711 user accounts allowing access to Nevada MMIS, including Division and non-Division state employees and fiscal agent employees.

Background Investigations Not Verified or Documented

The Division did not verify or document background investigations were performed for non-Division state employees and Division IT contractors that were granted access to MMIS. Non-Division state employees include employees from other state agencies like the Attorney General's Office or the Division of Child and Family Services that require access to the MMIS to perform job related duties. As state employees, these individuals may or may not have undergone background investigations prior to employment, but this was not verified by the Division.

Division staff indicated they do not have a process for verifying background investigations of employees of other agencies. As of June 2021, 84 active and former non-Division state employees had access to the MMIS.

In addition, the Division did not document a background investigation was performed for IT contractors. We randomly selected 7 of the Division's 13 IT contractors for testing. For four (57%) contractors tested, the Division had no record a background investigation was conducted.

State security standards require that fingerprint-based background investigations be conducted on state employees and IT contractors who work for or provide IT services to the State. Although the Division's policies outline a process for verifying contractors passed an appropriate background check prior to granting MMIS access, this process was not followed.

System User Accounts Created Before Background Investigation

Two of 10 (20%) fiscal agent user accounts tested were enabled in MMIS prior to the background investigation process being initiated and authorized by the Division. We judgmentally selected 10 newly hired employees of the 377 fiscal agent user accounts and tested when the background investigation packet was submitted to the Division. One account was created 12 days prior to the packet being submitted or approved. The documented background investigation procedure for the fiscal agent states that access to Nevada systems or data cannot be granted until background investigations are received and authorized by the Division Information Security Officer.

The Division's IT staff manage the background investigation process for individuals employed by the fiscal agent. IT staff verify a preliminary background check, or national records check, is performed before approving access to MMIS while awaiting the results of the fingerprint background investigation. However, the fiscal agent oversees granting access to MMIS for all system users, including their own. The Division has no way of knowing when new users are given access to MMIS other than when a background investigation packet is received from the fiscal agent.

Background investigations help identify and control who has access to information technology resources as well as establish an applicant's character and minimum qualifications for access to sensitive information. The Nevada MMIS contains electronic health information; therefore, background investigations help protect patients' sensitive, personal information from access by disreputable individuals.

Preliminary Background Investigations Not Performed

The Division's new employees are given system access prior to receiving a preliminary background investigation. As of June 2021, the Division had 237 active MMIS users. For all six newly hired Division employees in fiscal year 2021, access was granted to MMIS prior to completing a preliminary background investigation or fingerprint background investigation. A preliminary background investigation consists of a national records check while awaiting the results of a fingerprint-based investigation. A national records check provides detailed background information based on someone's name and Social Security number.

The average time the six employees had access to MMIS prior to receiving fingerprint background investigation results was approximately 37 days. One newly hired employee had access to MMIS for 61 days before results were received for the fingerprint background investigation.

State security standards indicate a national records check can be conducted if interim access is necessary before receiving the background investigation results. However, the Division's policies and procedures do not address performing a national records check when system access is needed before the results of the fingerprint background check are received.

Recommendations

1. Improve policies and procedures to ensure background investigations are performed and documented for Division IT contractors and employees of other state agencies prior to granting users access to MMIS.
2. Work with the fiscal agent to develop a process that will ensure background investigation packets and Division approval are received prior to creating user accounts in MMIS.
3. Revise Division new hire policies and procedures to ensure a national records check is completed, or background investigation results are received prior to granting users access to MMIS.

Division Oversight of System Users Can Be Improved

The Division does not actively manage MMIS user accounts. Specifically, the Division does not ensure MMIS access is still needed for non-Division state employees. In addition, the Division does not ensure that user accounts of former state employees and its fiscal agent are disabled timely. Finally, the Division does not ensure documentation used to authorize user MMIS access is complete or reviewed periodically. Accounts still valid after a user leaves an enterprise make it easier for an external or internal threat actor to gain unauthorized access to enterprise data using valid user credentials.

Inadequate Monitoring of User Accounts

During the audit, we identified several user accounts that have never been used, that have not been used for years, or remained active after the employee terminated service with the State. For 11 of 79 (14%) non-Division state employee MMIS user accounts tested, the employee had never logged into MMIS since being given access. The average duration the accounts remained enabled without logging in was 1.5 years as of November 2021. Three accounts remained enabled over 2 years without any login activity.

We also analyzed the login dates for other non-Division state employees whose last login date was before we requested a list of active user accounts in June 2021. Based on our analysis, nine other employees last recorded login to MMIS was before June 2021, and the average duration since the last time they logged in was 1.5 years. One employee had not logged into MMIS for over 2.5 years.

In addition, we identified four state employees that ended employment before June 30, 2021, their user accounts remained active for months after they terminated employment with the State.

Three of the termed employees' accounts remained active an average of 3 months, while the fourth user account was still active 8 months after terminating employment.

The Division does not have a process to actively monitor non-Division state employee user accounts and ensure system access is still needed. Instead, the Division relies on other state agencies and the fiscal agent to notify them when access is no longer needed.

In addition to termed state employees, we tested accounts of all seven fiscal agent users who were identified as terminated. One account was disabled the same day of termination while five remained enabled for several days. However, one of the accounts was enabled for over 2 months after the termination date. Since bringing this to the fiscal agent's attention, all terminated employees' accounts have been disabled.

It is easier for an external or internal threat actor to gain unauthorized access to enterprise assets or data through using valid user credentials than through "hacking" the environment. There are many ways to covertly obtain access to user accounts, including: accounts still valid after a user leaves the enterprise, dormant or lingering test accounts, or shared accounts that have not been changed in months or years. Account logging and monitoring is a critical component of security operations.

State security standards indicate that access rights for every State system shall be reviewed in the event of a change of access, whether by termination of contract, employment, or service. The Division has a policy that requires IT staff to disable a user account within 24 hours of notification. However, this policy does not address timely notification of IT staff. In addition, the policy does not address reviewing user accounts to determine if access is still required.

Documentation of User Access Authorizations Was Incomplete

The Division did not properly document system access authorization or documentation was inaccurate on the security access request (SAR) form, which is used to grant access to MMIS. A SAR form contains details of an employee or contractor requesting access to Division resources. The form includes the employee's name, agency, resources or permissions being requested, and documents appropriate approvals. Properly implemented and managed access controls to create, assign, manage, and revoke user access credentials and privileges are an important tool for controlling access to sensitive data.

We judgmentally selected 23 of the 334 non-fiscal agent user accounts for testing. We selected one account from each role group in MMIS. A role group defines how different users access different records in a system. In our review of the SAR form associated with these user accounts, we observed the following discrepancies between the form and access given in MMIS for state employees or IT contractors:

- Twelve forms did not have documentation of supervisor approval for access;
- Six forms did not have documentation of Information Security Officer approval for access;
- Five forms did not indicate the user's role; and
- Two had different roles in the system compared to the approved role on the SAR form.

In addition, the Division could not provide a SAR form for three users.

The Division did not follow its documented procedure for MMIS account review, which is to compare roles and account status with the SAR form on file. To verify users in the system, the procedure also requires a routine reconciliation of the user role and account status with the SAR form on file. Had the Division followed this procedure it would have identified and corrected the inaccurate and missing documentation.

Recommendations

4. Develop a policy and procedure requiring timely notification, by all entities with MMIS user accounts, of changes to user employment status or access needs.
5. Establish a process to review quarterly the status of all user accounts in MMIS, verify authorized roles, and to coordinate with other entities to identify unneeded accounts and disable access when no longer required.
6. Follow established procedures for MMIS account reconciliation with the properly completed SAR form on file and routinely review all user roles.

Medicaid Management Information System Enhancement Process Is Effective

The Division's Medicaid Management Information System (MMIS) enhancement process is effective in ensuring changes to the system are prioritized and completed. A documented change management plan is utilized and monitored. In addition, the Division monitors hours charged to individual enhancement projects. Proper management of this process helps ensure changes to the MMIS meet the needs of the project stakeholders and align with available resources.

Change Management Plan

A documented change management plan is utilized and monitored when enhancements to MMIS are needed. Changes to the MMIS are requested due to policy changes, initiatives, or Centers for Medicare and Medicaid Services required changes. For example, a change request could be updating the system to send automatic email notifications to providers or to ensure provider billings comply with the State Medicaid plan.

The Division utilizes a project management tool to create, track, and modify enhancement requests for the MMIS. For fiscal year 2021, there were 23 closed enhancements. Each enhancement request becomes a project with a contract and approved hours. The Division uses a prioritization method which assigns a high, normal, or low priority level to all projects and assigns a project manager to closely monitor the status of each project. We evaluated the enhancement projects and determined they are prioritized and completed in order of priority. Following its documented change management plan helps the Division identify, prioritize, and complete important enhancements to the MMIS, using available resources.

Monitoring of Enhancement Project Hours

The Division monitors hours charged to enhancement projects. We reviewed the fiscal agent contract and compared reports and invoices to ensure enhancement billings were reasonable. We assessed hours billed for enhancement projects including administrative hours. According to the contract, and confirmed during the audit, the fiscal agent submits a report monthly to the Division capturing time spent by engineers and business analysts performing enhancement work. The Division participates in monthly meetings with the fiscal agent to review project status.

During the audit, we requested the monthly reports, for fiscal year 2021, used to bill fiscal agent hours for enhancement projects. To ensure these billings were reasonable for the 12 months of the fiscal year, we compared the reports with the invoices and observed no significant errors. In addition, we judgmentally selected 5 of 11 high priority enhancement projects, completed during fiscal years 2020 and 2021, for testing. Our testing found all five projects were completed within the project budget. Based on our testing, the Division's process for monitoring helps ensure hours billed for enhancement projects are accurate and needed system enhancements are completed with available resources.

Appendix A
Audit Methodology

To gain an understanding of the Division of Health Care Financing and Policy (Division), we interviewed management, information technology (IT) support staff, and employees of the Division's IT contractor (fiscal agent) that maintains its Medicaid Management Information System (MMIS). Through discussions and a review of associated documents, we gained a broad understanding of how the MMIS is managed. In addition, we reviewed the State Information Security Policies, Standards, and Procedures; best practices from the Center for Internet Security Controls and the National Institute of Standards and Technology; and Nevada Administrative Code. We also reviewed the change management plan for operations, fiscal agent contract, financial information, budgets, and other information describing the Division's activities. Furthermore, we documented and assessed internal controls over the MMIS background check, user management, and system enhancement processes.

Our audit included a review of the Division's internal controls significant to our audit objective. Internal control is a process effected by an entity's oversight body, management, and other personnel that provides reasonable assurance that the objectives of an entity will be achieved. Internal control comprises the plans, methods, policies, and procedures used to fulfill the mission, strategic plan, goals, and objectives of the entity. The scope of our work on controls related to user access controls and MMIS change management system included the following:

- Design of control activities (Control Activities);
- Performance of monitoring activities and evaluation of issues and remediate deficiencies (Monitoring); and
- Exercise oversight responsibility (Control Environment).

Deficiencies and related recommendations to strengthen the Division's internal control systems are discussed in the body of the report. The design, implementation, and ongoing compliance with internal controls is the responsibility of agency management.

For our testing, we requested and reviewed a list of the active MMIS user accounts as of June 8, 2021. This list was used to test the Division and fiscal agents' background check and user access control processes. We assessed the completeness of this list by comparing it to a list of state employees in the State's Human Resource Database and through our testing of background check packets for fiscal agent employees.

To determine if the Division performed background checks on its new employees, IT contractors, and fiscal agent employees before granting them access to the MMIS, we judgmentally selected 10 of 377 fiscal agent users based on the most recent hire dates. In addition, we randomly selected 7 of 13 state IT contractors for testing. Furthermore, we judgmentally selected 6 of 237 Division users based on the most recent hire dates. For all individuals selected, we requested their background check packets and system access creation documentation. We reviewed this information to verify a national records check or fingerprint background check was performed, and that prior system access was not granted. Finally, we requested background investigation documentation regarding the 84 active and former non-Division state employees.

To determine if the Division actively manages user accounts in the MMIS, we obtained a report of the last login dates for active users and identified who had never logged into the system. In addition, we identified those users whose last log in was before June 2021 and calculated the time lapse since the last log in.

To verify the state MMIS users' employment status we queried the State's Human Resources Data Warehouse to determine if state employees who have access to the MMIS were still employed. Furthermore, we compared their termination dates with the MMIS system status and last modified dates to determine if those user accounts were disabled.

To verify fiscal agent MMIS users' employment status we requested the start and termination dates of those included on the user account list. Then, we compared those dates against the MMIS access creation date and last modified date to determine if the fiscal agent employees who have access to the MMIS were still employed.

To test user access controls, we separated the list of MMIS users into state and fiscal agent users, including Division IT contractors, and checked the list for record completeness to determine if the users' records were missing any user attributes. We also judgmentally selected one state user from each of the 23 user role groups based on the first name listed for that group. Then, we requested their system access request forms to verify if those forms were used, complete, and accurate. In addition, we judgmentally selected 10 fiscal agent users by sorting and selecting the first 10 fiscal agent employees based on the order of how they appeared on the list, requested their system access request forms, and verified if those forms were used, complete, and accurate.

To determine if the Division has adequate controls to monitor its MMIS change management process, we requested and reviewed a list of all enhancement projects for fiscal years 2020 and 2021, identified canceled projects, on-hold projects, and their associated priority levels to verify they were managed accordingly. In addition, we reviewed the reconciliation process used by the Division to verify all monthly fiscal year 2021 enhancement project hours billed by the fiscal agent agreed to supporting documentation. Finally, we judgmentally selected 5 of the 11 enhancement projects completed in fiscal years 2020 and 2021 based on total project hours and requested supporting documentation to verify that the hours billed to the project agreed to the approved hours.

We used nonstatistical audit sampling for our audit work, which was the most appropriate and cost-effective method for concluding on our audit objective. Based on our professional judgment, review of authoritative sampling guidance, and careful consideration of underlying statistical concepts, we believe that nonstatistical sampling provided sufficient, appropriate audit evidence to support the conclusions in our report. We did not project exceptions to the population because the nature of the testing did not lend itself to projecting to the population.

Our audit work was conducted from July 2020 to December 2021. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

In accordance with NRS 218G.230, we furnished a copy of our preliminary report to the Administrator of the Division of Health Care Financing and Policy. On February 22, 2022, we met with agency officials to discuss the results of the audit and requested a written response to the preliminary report. That response is contained in Appendix B, which begins on page 17.

Contributors to this report included:

Shirlee Eitel-Bingham, CISA
Deputy Legislative Auditor

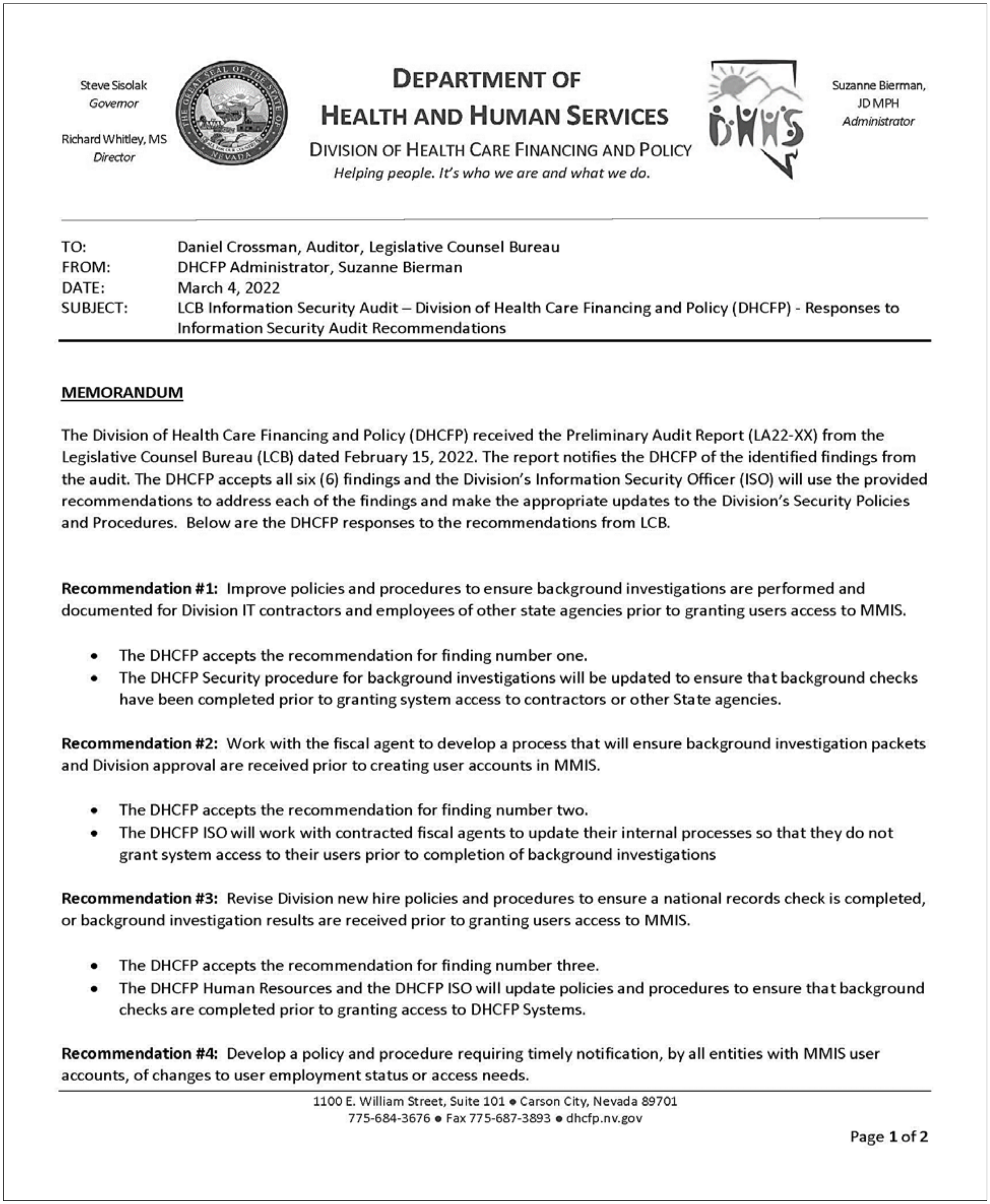
Christopher Gray, MPA
Deputy Legislative Auditor

Todd C. Peterson, MPA
Audit Supervisor

Shannon Riedel, CPA
Chief Deputy Legislative Auditor

Appendix B

Response From the Division of Health Care Financing and Policy



Steve Sisolak
Governor

Richard Whitley, MS
Director

DEPARTMENT OF
HEALTH AND HUMAN SERVICES
DIVISION OF HEALTH CARE FINANCING AND POLICY
Helping people. It's who we are and what we do.

Suzanne Bierman,
JD MPH
Administrator

TO: Daniel Crossman, Auditor, Legislative Counsel Bureau
FROM: DHCFP Administrator, Suzanne Bierman
DATE: March 4, 2022
SUBJECT: LCB Information Security Audit – Division of Health Care Financing and Policy (DHCFP) - Responses to Information Security Audit Recommendations

MEMORANDUM

The Division of Health Care Financing and Policy (DHCFP) received the Preliminary Audit Report (LA22-XX) from the Legislative Counsel Bureau (LCB) dated February 15, 2022. The report notifies the DHCFP of the identified findings from the audit. The DHCFP accepts all six (6) findings and the Division's Information Security Officer (ISO) will use the provided recommendations to address each of the findings and make the appropriate updates to the Division's Security Policies and Procedures. Below are the DHCFP responses to the recommendations from LCB.

Recommendation #1: Improve policies and procedures to ensure background investigations are performed and documented for Division IT contractors and employees of other state agencies prior to granting users access to MMIS.

- The DHCFP accepts the recommendation for finding number one.
- The DHCFP Security procedure for background investigations will be updated to ensure that background checks have been completed prior to granting system access to contractors or other State agencies.

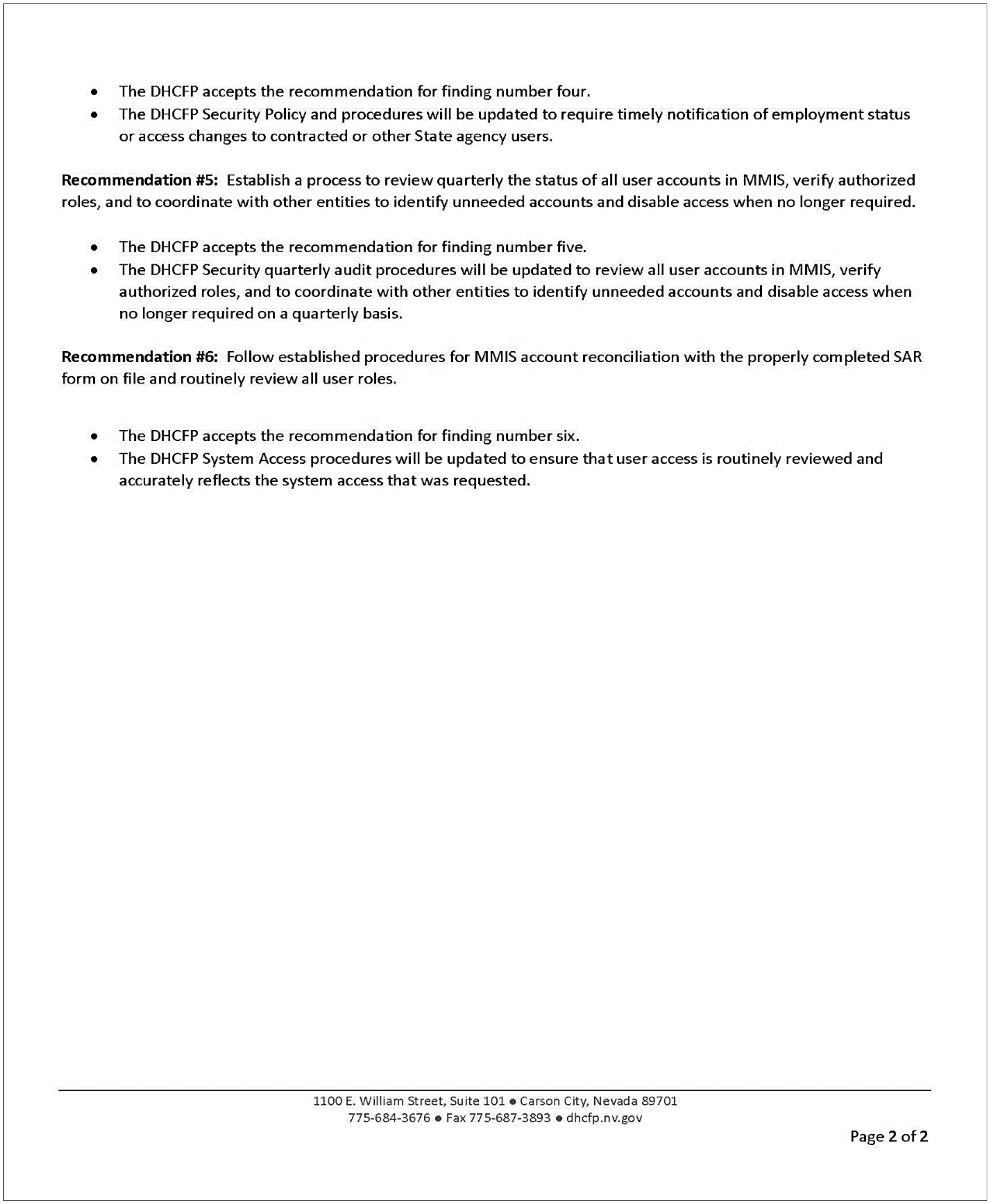
Recommendation #2: Work with the fiscal agent to develop a process that will ensure background investigation packets and Division approval are received prior to creating user accounts in MMIS.

- The DHCFP accepts the recommendation for finding number two.
- The DHCFP ISO will work with contracted fiscal agents to update their internal processes so that they do not grant system access to their users prior to completion of background investigations

Recommendation #3: Revise Division new hire policies and procedures to ensure a national records check is completed, or background investigation results are received prior to granting users access to MMIS.

- The DHCFP accepts the recommendation for finding number three.
- The DHCFP Human Resources and the DHCFP ISO will update policies and procedures to ensure that background checks are completed prior to granting access to DHCFP Systems.

Recommendation #4: Develop a policy and procedure requiring timely notification, by all entities with MMIS user accounts, of changes to user employment status or access needs.



- The DHCFP accepts the recommendation for finding number four.
- The DHCFP Security Policy and procedures will be updated to require timely notification of employment status or access changes to contracted or other State agency users.

Recommendation #5: Establish a process to review quarterly the status of all user accounts in MMIS, verify authorized roles, and to coordinate with other entities to identify unneeded accounts and disable access when no longer required.

- The DHCFP accepts the recommendation for finding number five.
- The DHCFP Security quarterly audit procedures will be updated to review all user accounts in MMIS, verify authorized roles, and to coordinate with other entities to identify unneeded accounts and disable access when no longer required on a quarterly basis.

Recommendation #6: Follow established procedures for MMIS account reconciliation with the properly completed SAR form on file and routinely review all user roles.

- The DHCFP accepts the recommendation for finding number six.
- The DHCFP System Access procedures will be updated to ensure that user access is routinely reviewed and accurately reflects the system access that was requested.

Division of Health Care Financing and Policy's Response to Audit Recommendations

	Recommendations	Accepted	Rejected
1.	Improve policies and procedures to ensure background investigations are performed and documented for Division IT contractors and employees of other state agencies prior to granting users access to MMIS	X	
2.	Work with the fiscal agent to develop a process that will ensure background investigation packets and Division approval are received prior to creating user accounts in MMIS..	X	
3.	Revise Division new hire policies and procedures to ensure a national records check is completed, or background investigation results are received prior to granting users access to MMIS...	X	
4.	Develop a policy and procedure requiring timely notification, by all entities with MMIS user accounts, of changes to user employment status or access needs...	X	
5.	Establish a process to review quarterly the status of all user accounts in MMIS, verify authorized roles, and to coordinate with other entities to identify unneeded accounts and disable access when no longer required..	X	
6.	Follow established procedures for MMIS account reconciliation with the properly completed SAR form on file and routinely review all user roles	X	
	TOTALS	6	