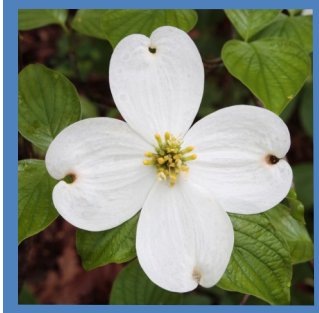



# DEPARTMENT OF MEDICAL ASSISTANCE SERVICES

## REPORT ON AUDIT FOR THE YEAR ENDED JUNE 30, 2024

Auditor of Public Accounts
Staci A. Henshaw, CPA
www.apa.virginia.gov
(804) 225-3350

## AUDIT SUMMARY

Our audit of the Department of Medical Assistance Services (Medical Assistance Services), including the Medicaid Cluster and Coronavirus State and Local Fiscal Recovery Funds federal grant programs, for the fiscal year ended June 30, 2024, found:

- proper recording and reporting of all transactions, in all material respects, in the Commonwealth's accounting and reporting system, Medical Assistance Services' financial systems, and supplemental information and attachments submitted to the Department of Accounts;

- five matters, one of which is a material weakness, involving internal control and its operation necessary to bring to management's attention that also represent instances of noncompliance with applicable laws and regulations or other matters that are required to be reported; and

- adequate corrective action with respect to prior audit findings and recommendations identified as complete in the Findings Summary included in the Appendix.

In the section titled "Internal Control and Compliance Findings and Recommendations," we have included our assessment of the conditions and causes resulting in the internal control and compliance findings identified through our audit as well as recommendations for addressing those findings. Our assessment does not remove management's responsibility to perform a thorough assessment of the conditions and causes of the findings and develop and appropriately implement adequate corrective actions to resolve the findings as required by the Department of Accounts in Topic 10205 – Agency Response to APA Audit of the Commonwealth Accounting Policies and Procedures Manual. Those corrective actions may include additional items beyond our recommendations.

Additionally, our report includes two risk alerts that require the action and cooperation of Medical Assistance Services' management and the Virginia Information Technologies Agency (VITA) regarding risks related to unpatched software and access to centralized audit log information.

In fiscal year 2023, we included the results of our audit over Medical Assistance Services in the report titled "Agencies of the Secretary of Health and Human Resources for the year ended June 30, 2023."

# -TABLE OF CONTENTS-

# INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS

## Improve Information Security Program and Controls

**Type:** Internal Control and Compliance
**Severity:** Material Weakness
**First Reported:** Fiscal Year 2020

Medical Assistance Services continues to address weaknesses in its information technology (IT) general controls originally identified in a 2020 audit and confirmed in a 2023 audit covering the same IT general controls conducted by Medical Assistance Services' Internal Audit division. During the 2023 audit, Internal Audit tested 105 controls required by the Commonwealth's previous version of the Information Security Standard, SEC501, and identified 61 individual control weaknesses, a 58% non-compliance rate, that Internal Audit grouped into eight findings. Medical Assistance Services addressed four of the eight findings during fiscal year 2024.

Noncompliance with required security controls increases the risk for unauthorized access to mission-critical systems and data in addition to weakening Medical Assistance Services ability to respond to malicious attacks to its IT environment. Medical Assistance Services has experienced delays in addressing these findings due to the number of findings and resources required to remediate the weaknesses. Medical Assistance Services updated its corrective action plan for the four remaining findings in June 2024, stating corrective actions are still ongoing with an estimated completion date of September 2024.

Medical Assistance Services should prioritize and dedicate the necessary resources to ensure timely completion of its corrective action plans and to become compliant with the current version of the Commonwealth's Information Security Standard, SEC530 (Security Standard). These actions will help maintain the confidentiality, integrity, and availability of sensitive and mission-critical data.

## Improve Fiscal Agent Oversight

**Type:** Internal Control and Compliance
**Severity:** Significant Deficiency

Medical Assistance Services did not obtain and review a System and Organization Controls (SOC) report, specifically a SOC I, Type 2 report, to gain assurance over its fiscal agent's internal controls relevant to financial reporting. In addition to services related to information systems management and security, Medical Assistance Services contracts with the fiscal agent to perform accurate and timely payments of Medicaid claims to providers and maintain an accounts receivable ledger for the collection of provider funds owed to Medical Assistance Services. The fiscal agent processed over $22 billion in Medicaid-related payments during fiscal year 2024.

Medical Assistance Services obtained a SOC 2, Type 2 report related to the fiscal agent's controls over information systems management and security, however, this report did not provide an opinion over internal controls relevant to Medical Assistance Services' significant fiscal activity and financial

reporting. The Commonwealth's Accounting Policies and Procedures Manual Topic 10305 requires agencies to have adequate interaction with service providers to appropriately understand the service provider's internal control environment. It also states that agencies must also maintain oversight over service providers to gain assurance over outsourced operations. Additionally, Title 2 U.S. Code of Federal Regulations (CFR) § 200.303(a) requires non-federal entities to establish and maintain effective internal control over the federal award that provides reasonable assurance that the non-federal entity is managing the federal award in compliance with federal statutes, regulations, and the terms and conditions of the federal award.

The existing contract between Medical Assistance Services and the fiscal agent does not require the fiscal agent to obtain an independent review opining to the effectiveness of internal controls related to Medical Assistance Services' significant fiscal activities and financial reporting. Management asserted that they are currently working to modify the contract with the provider to add this requirement. Although management maintains a high degree of interaction with its fiscal agent, they cannot adequately ensure the fiscal agent has designed and implemented sufficient controls, and whether the controls are operating effectively without obtaining and reviewing a SOC I, Type 2 report. This issue increases the risk that management will not detect a weakness in the fiscal agent's environment, which could negatively impact the Commonwealth.

Medical Assistance Services should continue to work with the fiscal agent to add language to the contract that would require the fiscal agent to obtain an appropriate independent audit of its internal controls relevant to Medical Assistance Services' financial activities and reporting. Once the new contract language is in effect, Medical Assistance Services' management should obtain and review the SOC I, Type 2 report annually to ensure the fiscal agent is meeting contractual obligations and has proper internal controls over Medical Assistance Services' significant fiscal activities and financial reporting.

**Improve Database Security**

**Type:** Internal Control and Compliance
**Severity:** Significant Deficiency

Medical Assistance Services does not have formal policies, procedures, and a baseline configuration that outlines requirements and justifications for securing and maintaining the database supporting its primary system for financial accounting and reporting operations in accordance with the Security Standard, and industry best practices, such as the Center for Internet Security Benchmarks (CIS Benchmark). As a result, Medical Assistance Services has not implemented some required controls over the database. We communicated the weaknesses to management in a separate document marked Freedom of Information Act Exempt (FOIAE) under § 2.2-3705.2 of the Code of Virginia due to it containing descriptions of security mechanisms.

The Security Standard requires Medical Assistance Services to develop, document, and disseminate information security policies and procedures that align with the control requirements in the Security Standard. Additionally, the Security Standard requires Medical Assistance Services to develop, document, and maintain a current baseline configuration of the system and apply more restrictive security configurations for sensitive systems. The Security Standard also requires Medical Assistance

Services to review and update the policies, procedures, and baseline configuration on an annual basis and following an environmental change.

Without detailed policies, procedures, and a baseline configuration that outlines requirements and justifications for securing and maintaining its database, Medical Assistance Services increases the risk that the system will not meet the minimum security requirements and recommendations to protect its sensitive data from malicious parties. Medical Assistance Services has experienced a lack of resources which has contributed to the absence of documentation outlining control requirements and procedures needed to properly secure the database. The absence of this documentation contributed to the deficiencies communicated in the FOIAE document and as a result, Medical Assistance Services has not consistently evaluated and applied security controls.

Medical Assistance Services should dedicate the resources necessary to develop and implement formal policies and procedures to support its database based on the Security Standard requirements and settings recommended by industry best practices, such as the CIS Benchmark. Medical Assistance Services should develop a formal baseline configuration for the database that defines required security controls outlined in industry best practices, such as the CIS Benchmark. The baseline configuration should define deviations from recommended and expected security configurations as well as business justification and approval for any deviations. Additionally, Medical Assistance Services should develop a process to review the database's configuration against its established baseline configuration on a scheduled basis and after major changes occur to help detect and address potential misconfigurations timely. Furthermore, Medical Assistance Services should implement the security controls and processes communicated in the FOIAE document to address risks present in the database to ensure the configuration aligns with the Security Standard and CIS Benchmark. These actions will help maintain the confidentiality, availability, and integrity of Medical Assistance Services' sensitive and mission-critical data.

**Improve Vulnerability Remediation Efforts**

**Type:** Internal Control and Compliance
**Severity:** Significant Deficiency

Medical Assistance Services does not install security patches to mitigate vulnerabilities within its IT environment in accordance with its Vulnerability Scan Management procedure. Specifically, as of November 2024, Medical Assistance Services identified a significant number of vulnerabilities classified with a severity of critical and high and numerous vulnerabilities with a severity of medium or low in its IT environment that remained unmitigated beyond the time limits set in its procedure.

Medical Assistance Services' procedure requires the agency to mitigate and validate vulnerabilities within the following timeframes, depending on the vulnerability's severity rating:

- High-severity flaws within 30 calendar days;
- Medium-severity flaws within 60 calendar days; and
- All others within 90 calendar days.

Additionally, the Security Standard requires Medical Assistance Services to "monitor and scan for vulnerabilities in the system and hosted applications at least once every 30 days, and when new vulnerabilities potentially affecting the system are identified and reported." The Security Standard also requires Medical Assistance Services to remediate legitimate vulnerabilities within 30 days unless otherwise specified by Commonwealth Security Risk Management (CSRM) in accordance with an organizational assessment of risk. The Commonwealth's IT Risk Management Standard, SEC520 (Risk Management Standard) requires Medical Assistance Services to "fix vulnerabilities within 30 days of a fix becoming available that are either rated as critical or high according to the National Vulnerability Database or otherwise identified by CSRM." Additionally, the Risk Management Standard requires Medical Assistance Services to remediate all other vulnerabilities within 90 days of a fix becoming available and acquire an approved security exception for the vulnerability should Medical Assistance Services not remediate it within the timeframes identified.

Software vulnerabilities are publicly known flaws that bad actors may exploit and use to circumvent organizational information security controls to infiltrate a network or application. The longer these vulnerabilities exist in an environment, the higher the risk of a compromise and unauthorized access to sensitive and mission-critical systems and data. It is therefore imperative for organizations to respond quickly and mitigate these publicly known flaws as soon as possible. Without appropriate software patching and vulnerability management controls, Medical Assistance Services increases the risk of unauthorized access to sensitive and mission-critical systems. Medical Assistance Services lacks the staffing necessary to remediate the high number of vulnerabilities detected within the timeframes required by its Vulnerability Scan Management procedure.

Medical Assistance Services should allocate the necessary resources to apply patches within the Vulnerability Scan Management procedure's required timeframe to mitigate the vulnerabilities affecting its IT environment. If Medical Assistance Services is unable to mitigate vulnerabilities within the required timeframe, it should obtain an extension approval from CSRM that is based on an organizational assessment of risk. Timely remediation of significant vulnerabilities will help protect the confidentiality, integrity, and availability of Medical Assistance Services' sensitive and mission-critical information.

**Improve IT Third-Party Oversight Process**

**Type:** Internal Control and Compliance
**Severity:** Significant Deficiency
**First Issued:** Fiscal Year 2022

Medical Assistance Services has made progress to document and implement a formal process for maintaining oversight for three of its IT third-party service providers that manage and support its Medicaid management system. The Medicaid management system encompasses different functions, such as member and provider reporting, financial reporting, and federal reporting.

Since the prior year audit, Medical Assistance Services developed its Information Technology (IT) Third Party Risk Management Procedure, which was effective on February 1, 2024, to facilitate the implementation of its IT System and Services Acquisition Policy. However, Medical Assistance Services is still working to implement the new procedure, which has resulted in the agency not yet verifying the

following required controls and processes for one of the Medicaid management system IT service providers that is not covered by the Virginia Information Technologies Agency (VITA) Commonwealth of Virginia Risk and Authority Management Program.

- Medical Assistance Services does not confirm the geographic location of sensitive data monthly for IT service providers. Without confirming the geographic location of sensitive data, Medical Assistance Services may be unable to enforce contract requirements, laws, and standards due to the data falling outside of the United States' jurisdiction.

- Medical Assistance Services does not confirm whether IT service providers perform vulnerability scans every 90 days. By not obtaining and analyzing the vulnerability scan results from the IT service provider, Medical Assistance Services increases the risk that the IT service providers are not remediating legitimate vulnerabilities in a timely manner.

Medical Assistance Services experienced delays in implementing its new procedure due to limited staffing to properly communicate and train those responsible for monitoring IT service providers. Medical Assistance Services expects to complete its implementation by October 2024. Medical Assistance Services should dedicate the resources necessary to finish implementing its Third-Party Risk Management Procedure. Additionally, Medical Assistance Services should ensure that those tasked with monitoring IT service providers are confirming the geographic location of sensitive data and the provider's performance of vulnerability scanning and remediation efforts per the Security Standard. Medical Assistance Services should also ensure the individuals responsible for monitoring consistently perform formal oversight processes in a timely manner, which will help maintain the confidentiality, integrity, and availability of sensitive and mission-critical data.

## RISK ALERTS

During our audit, we encountered issues that are beyond the corrective action of Medical Assistance Services' management alone and which require the action and cooperation of management and VITA. The following issues represent such a risk to Medical Assistance Services and the Commonwealth.

**Unpatched Software**

**First Reported:** Fiscal Year 2021

VITA contracts with various providers to create the Commonwealth's Information Technology Infrastructure Services Program (ITISP) to provide agencies with installation, maintenance, operation, and support of IT infrastructure components, such as servers, routers, firewalls, and virtual private networks. Medical Assistance Services continues to rely on contractors procured by VITA for the installation of security patches in systems that support Medical Assistance Services' operations. Additionally, Medical Assistance Services relies on VITA as the contract administrator to maintain oversight and enforce the contract agreements with the ITISP contractors. As of November 2024, the ITISP contractors had not applied a significant number of security patches that are critical and highly important to Medical Assistance Services' IT infrastructure components, all of which are past the 30-day update window allowed by the Security Standard.

The Security Standard requires the installation of security-relevant software and firmware updates within 30 days of release or within a timeframe approved by VITA's CSRM division. The Security Standard does allow for varying time periods depending on factors such as the criticality of the update, but generally the ITISP uses a 30-day window from the date of release as its standard for determining timely implementation of security patches. Missing system security updates increase the risk of successful cyberattack, exploit, and data breach by malicious parties.

While VITA is responsible for enforcing the service level agreement, it has not been able to compel the current ITISP contractors to install certain security patches to Medical Assistance Services' IT infrastructure to remediate vulnerabilities in a timely manner or take actions to obtain these required services from another source. Medical Assistance Services is working with VITA and the ITISP contractors to ensure that the ITISP contractors install all critical and highly important security patches on all servers. Our separate audit of VITA's contract management will also continue to report this issue.

**Access to Centralized Audit Log Information**

**First Reported:** Fiscal Year 2021

Medical Assistance Services relies on the Commonwealth's ITISP to install, maintain, operate, and support IT infrastructure components, such as servers, routers, firewalls, and virtual private networks. As part of these services, Medical Assistance Services relies on contractors procured by VITA to provide Medical Assistance Services access to a centralized monitoring tool, known as the Managed, Detection, Response (MDR) Dashboard, that collects audit log information about activities in Medical Assistance Services' IT environment so that Medical Assistance Services can review logged activity. Additionally,

Medical Assistance Services relies on VITA to maintain oversight and enforce the service level agreements and deliverables with the ITISP contractors.

While VITA did not originally enforce the deliverable requirement when ratifying the ITISP contracts in 2018, VITA tried to compel the ITISP contractor to grant agencies, such as Medical Assistance Services, access to the monitoring tool and audit log information for the last five years. The MDR Dashboard went live in October 2023 but did not include all audit log information to allow agencies to adequately monitor their IT environments. Additionally, VITA implemented a separate security and event management (SIEM) tool at the end of October 2023 to expand agencies' capabilities to monitor audit log information. As of October 2024, VITA and the ITISP supplier determined the MDR Dashboard will be replaced by the VITA-managed SIEM tool as the permanent audit log monitoring tool. However, while the VITA-managed SIEM tool is in production, it also does not include all audit log information in a usable format to allow agencies to adequately monitor their IT environments.

The Security Standard requires a review and analysis of audit records at least every 30 days for indications of inappropriate or unusual activity and assessment of the potential impact of the inappropriate or unusual activity. Using a SIEM tool without all necessary audit log information reduces organizational security posture by not being able to react to and investigate suspicious system activity in a timely manner. Medical Assistance Services is working with VITA to import audit log information to the SIEM tool and provide feedback on its uses to ensure Medical Assistance Services can review the activities occurring in its IT environment in accordance with the Security Standard. Our separate audit of VITA's contract management will also continue to report this issue.

Commonwealth of Virginia

*Auditor of Public Accounts*

Staci A. Henshaw, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

December 13, 2024

The Honorable Glenn Youngkin
Governor of Virginia

Joint Legislative Audit
and Review Commission

Janet Kelly
Secretary of Health and Human Resources

Cheryl J. Roberts
Director, Department of Medical Assistance Services

We have audited the financial records, operations, and federal compliance of the **Department of Medical Assistance Services** (Medical Assistance Services), including federal programs as defined in the Audit Scope and Methodology section below, for the year ended June 30, 2024. We conducted this audit in accordance with auditing standards generally accepted in the United States of America and the standards applicable to financial audits contained in Government Auditing Standards, issued by the Comptroller General of the United States, in support of the Commonwealth's Annual Comprehensive Financial Report and Single Audit. 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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

## Audit Objectives

Our audit's primary objective was to evaluate the accuracy of Medical Assistance Services' financial transactions as reported in the Annual Comprehensive Financial Report for the Commonwealth of Virginia and test federal compliance in support of the Commonwealth's Single Audit for the year ended June 30, 2024. In support of this objective, we evaluated the accuracy of recorded financial transactions in the Commonwealth's accounting and financial reporting system, Medical Assistance Services' financial systems, and supplemental information and attachments submitted to the Department of Accounts; reviewed the adequacy of Medical Assistance Services' internal control; tested for compliance with applicable laws, regulations, contracts, and grant agreements; and reviewed corrective actions with respect to audit findings and recommendations from prior year reports.

## Audit Scope and Methodology

Medical Assistance Services' management has responsibility for establishing and maintaining internal control and complying with applicable laws, regulations, contracts, and grant agreements. Internal control is a process designed to provide reasonable, but not absolute, assurance regarding the reliability of financial reporting, effectiveness and efficiency of operations, and compliance with applicable laws, regulations, contracts, and grant agreements.

We gained an understanding of the overall internal controls, both automated and manual, sufficient to plan the audit. We considered materiality and risk in determining the nature and extent of our audit procedures. Our review encompassed controls over the following federal grant programs and the following significant cycles, classes of transactions, and account balances:

Accounts payable
Accounts receivable
Contract procurement and management
General Fund revenues (drug rebate) and expenses
Federal revenues, expenses, and compliance for the following federal grant programs:
- Medicaid Cluster
- Coronavirus State and Local Fiscal Recovery Funds

Provider assessment revenues and expenses
Information system security (including access controls)

We performed audit tests to determine whether Medical Assistance Services' controls were adequate, had been placed in operation, and were being followed. Our audit also included tests of compliance with provisions of applicable laws, regulations, contracts, and grant agreements. Our audit procedures included inquiries of appropriate personnel, inspection of documents, records, and contracts, and observation of Medical Assistance Services' operations. We performed analytical procedures, including budgetary and trend analyses, and tested details of transactions to achieve our audit objectives.

A nonstatistical sampling approach was used. Our samples were designed to support conclusions about our audit objectives. An appropriate sampling methodology was used to ensure the samples selected were representative of the population and provided sufficient, appropriate evidence. We identified specific attributes for testing each of the samples and, when appropriate, we projected our results to the population.

Our consideration of internal control over financial reporting and federal compliance (internal control) was for the limited purpose described in the section "Audit Objectives" and was not designed to identify all deficiencies in internal control that might be material weaknesses or significant deficiencies and therefore, material weaknesses or significant deficiencies may exist that were not identified. However, as described in the section titled "Internal Control and Compliance Findings and Recommendations," we identified certain deficiencies in internal control that we consider to be material weaknesses and significant deficiencies.

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct misstatements or noncompliance on a timely basis. A material weakness is a deficiency, or a combination of deficiencies, in internal control such that there is a reasonable possibility that a material misstatement of the entity's financial statements or material noncompliance with a type of compliance requirement of a federal program will not be prevented or detected and corrected on a timely basis. We consider the deficiency titled "Improve Information Security Program and Controls," which is described in the section titled "Internal Control and Compliance Findings and Recommendations," to be a material weakness.

A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance. We consider the remaining deficiencies described in the section titled "Internal Control and Compliance Findings and Recommendations," to be significant deficiencies.

## Conclusions

We found that Medical Assistance Services properly stated, in all material respects, the amounts recorded and reported in the Commonwealth's accounting and financial reporting system, Medical Assistance Services' financial systems, and supplemental information and attachments submitted to the Department of Accounts.

We noted certain matters involving internal control and its operation and compliance with applicable laws, regulations, contracts, and grant agreements that require management's attention and corrective action. These matters are described in the section titled "Internal Control and Compliance Findings and Recommendations."

Medical Assistance Services has taken adequate corrective action with respect to two prior audit findings identified as complete in the Findings Summary included in the Appendix.

Since the findings noted above include those that have been identified as material weaknesses and significant deficiencies, they will be reported as such in the "Independent Auditor's Report on Internal Control over Financial Reporting and on Compliance and Other Matters Based on an Audit of the Financial Statements Performed in Accordance with Government Auditing Standards" and the "Independent Auditor's Report on Compliance for Each Major Federal Program; Report on Internal Control over Compliance; and Report on Schedule of Expenditures of Federal Awards Required by Uniform Guidance," which are included in the Commonwealth of Virginia's Single Audit Report for the year ended June 30, 2024. The Single Audit Report will be available at www.apa.virginia.gov in February 2025.

## Exit Conference and Report Distribution

We discussed this report with management at an exit conference held on January 13, 2025. Government Auditing Standards require the auditor to perform limited procedures on Medical

Assistance Services' response to the findings identified in our audit, which is included in the accompanying section titled "Agency Response." Medical Assistance Services' response was not subjected to the other auditing procedures applied in the audit, and, accordingly, we express no opinion on the response.

This report is intended for the information and use of the Governor and General Assembly, management, and the citizens of the Commonwealth of Virginia and is a public record.

Staci A. Henshaw
AUDITOR OF PUBLIC ACCOUNTS

JDE/vks

## FINDINGS SUMMARY

| Finding Title | Status of Corrective Action* | First Reported for Fiscal Year |
|---|---|---|
| Obtain and Review Information Security Audit | Complete | 2023 |
| Perform Annual System Access Reviews | Complete | 2023 |
| Improve Information Security Program and Controls | Ongoing | 2020 |
| Improve Fiscal Agent Oversight | Ongoing | 2024 |
| Improve Database Security | Ongoing | 2024 |
| Improve Vulnerability Remediation Efforts | Ongoing | 2024 |
| Improve IT Third-Party Oversight Process | Ongoing | 2022 |

* A status of **Complete** indicates management has taken adequate corrective action. **Ongoing** indicates new and/or existing findings that require management's corrective action as of fiscal year end.

# COMMONWEALTH of VIRGINIA

***Department of Medical Assistance Services***

CHERYL J. ROBERTS
DIRECTOR

SUITE 1300
600 EAST BROAD STREET
RICHMOND, VA 23219
804/786-7933
804/343-0634 (TDD)
www.dmas.virginia.gov

January 15, 2025

Ms. Staci A. Henshaw, CPA
Auditor of Public Accounts
Commonwealth of Virginia
P. O. Box 1295
Richmond, Virginia 23218

Dear Ms. Henshaw:

We have reviewed the FY24 Audit Report for the Department of Medical Assistance Services (DMAS) for the Fiscal Year Ending June 30, 2024. We concur with the audit findings and will submit a response to the Department of Accounts, within the required thirty days after the report is issued. The response will include the work plans for corrective actions that DMAS will take to address the audit findings.

We appreciate the audit team's work and feedback. If you have any questions or require additional information, please contact the DMAS Internal Audit Director, Susan Smith.

Sincerely,

Cheryl J. Roberts, JD
Director