AGENCIES OF THE SECRETARY OF HEALTH AND HUMAN RESOURCES

REPORT ON AUDIT FOR THE YEAR ENDED JUNE 30, 2015

Auditor of Public Accounts
Martha S. Mavredes, CPA
www.apa.virginia.gov
(804) 225-3350

AUDIT SUMMARY

This report summarizes our fiscal year 2015 audit results for the four largest agencies under the Secretary of Health and Human Resources, which were tested for the Commonwealth's Comprehensive Annual Financial Report (CAFR) and Single Audit report.

Within this report are 38 findings, which are grouped by each agency and relate to internal controls and compliance, or both. Those findings that report on issues that were not resolved from our previous audit are designated with "REPEAT" at the end of their title. This report also contains some issues that are designated as Risk Alerts. These differ from internal control and compliance findings in that they represent an issue that is beyond the corrective action of the individual agency and requires the cooperation of others to address the risk.

Overall, our audit for the year ended June 30, 2015, found:

- proper recording and reporting of all transactions, in all material respects, in the Commonwealth Accounting and Reporting System and in each agency's accounting records;
- 37 matters involving internal control and its operation necessary to bring to management's attention;
- 36 instances of noncompliance with applicable laws and regulations or other matters that are required to be reported;
- 10 findings that were reported in the prior year and are classified in this report as repeat findings; and
- 2 items that are considered Risk Alerts.

Why the APA Audits These Four Agencies Every Year

Collectively the following four agencies spent $12 billion, or 96 percent, of the total funds expended by the agencies under the Secretary of Health and Human Resources:

- Department of Medical Assistance Services;
- Department of Social Services;
- Department of Behavioral Health and Developmental Services; and
- Department of Health.

–TABLE OF CONTENTS–

Risk Alert – Continue to Comply with the DOJ Settlement Agreement

During the course of our audit, we encountered issues that are beyond the corrective action of the Department of Behavioral Health and Developmental Services (DBHDS) management and require the action and cooperation of management, the General Assembly, and the Administration. The following issue represents such a risk to DBHDS and the Commonwealth.

In January of 2012, the Commonwealth of Virginia and the United States Department of Justice (DOJ) reached a settlement agreement to resolve a DOJ investigation of the Commonwealth's training centers and community programs under the jurisdiction of DBHDS. This settlement agreement also addressed the Commonwealth's compliance with both the Americans with Disabilities Act and the U.S. Supreme Court Olmstead ruling requiring individuals be served in the most integrated settings appropriate to meet their needs. The major highlights of the settlement include the expansion of community-based services through waiver slots; strengthened quality and risk management systems for community services, and the transitioning of affected individuals from the training centers to new homes in the community.

The Commonwealth continues to work with the Department of Justice and an independent reviewer to meet the terms of the settlement agreement. DBHDS plans to close four of its five training centers by 2020. Southside Virginia Training Center closed in May 2014. Northern Virginia Training Center, originally scheduled to close in June 2015, is now scheduled to close in March 2016. Southwest Virginia Training Center and Central Virginia Training Center will close in June 2018 and June 2020, respectively. The delay in closure of Northern Virginia Training Center has not had a negative effect on the settlement. However, there is a risk of future non-compliance if DBHDS does not receive adequate funding at the appropriate time for the transition programs and a stoppage of services results. Specifically, funds are needed:

- to address critical and ongoing one-time requirements to build community capacity as well as remain compliant with other aspects of the settlement agreement;

- to support facility transition waiver slots to enable DBHDS to move individuals out of the training centers and into community based programs, as well as additional community intellectual and developmental disability (ID/DD) waiver slots to help reduce the growing waiting list for services;

- to support individuals in community based programs with housing, transportation, and other services; and

- to maintain the certification staffing standards of training centers, due to delays in the projected discharge of individuals into the community, and/or the training centers remain open beyond their scheduled closure date due to unforeseen policy or operational considerations.

We encourage DBHDS, the General Assembly, and the Administration to work together to ensure that DBHDS has the funds and support it needs to continue to comply with the settlement agreement and provide services to individuals in the appropriate setting.

Why the APA Audits Information Systems Security

DBHDS collects, manages, and stores significant volumes of personal and financial data within its mission critical systems. Because of the highly sensitive and critical nature of this data, DBHDS management must take all necessary precautions to ensure the integrity and security of the data within its systems. To determine if database security, oversight of sensitive systems, and systems access was adequate, we compared the practices of DBHDS to those required by the Commonwealth's Information Security Standard.

Improve Information Technology Governance

Condition

DBHDS is not protecting sensitive Commonwealth data in accordance with the Commonwealth's standards and has an insufficient governance structure to manage its information security program. DBHDS has a decentralized information technology (IT) environment that allows the Central Office and 15 separate facilities to manage and maintain sensitive systems independently.

Due to the decentralized IT environment, DBHDS has 437 disparate sensitive systems at the Central Office and facilities, with multiple systems performing the same or similar business functions. For example, there are currently four Pharmacy Management Systems including the Electronic Health Records system, OneMind. DBHDS intends OneMind to be an enterprise solution; however, only two facilities are using it and there is no timetable or plan to implement OneMind at the other facilities because DBHDS lacks the IT resources and funding.

Having 437 sensitive systems requires extensive IT resources to ensure compliance with the agency's enterprise security program and the Commonwealth's Information Security Standard. Managing and maintaining 437 sensitive systems is not feasible with DBHDS' current resource levels, and DBHDS has no formal plan to consolidate the disparate systems performing similar business functions across the entire agency.

Criteria

The Commonwealth's Information Security Standard, SEC 501-09 (Security Standard), Section 2.4.2, requires the agency head to ensure that DBHDS maintains an information security program that is sufficient to protect the agency's IT systems and that is documented and effectively communicated.

In addition, DBHDS has control weaknesses in the following areas showing that DBHDS does not maintain appropriate oversight over its information security program and does not meet the requirements in the Security Standard:

- End-of-life technology;
- Risk management process;
- Vulnerability assessment process;
- Software baseline configurations;
- ISO reporting structure;
- Database security;
- Web application security; and
- Assurance over third-party providers.

Consequence

Not having an appropriate governance structure to properly manage the agency's IT environment and information security program can result in a data breach or unauthorized access to confidential and mission critical data leading to data corruption, data loss, or system disruption if accessed by a malicious attacker, either internal or external. If a breach occurs and Health Insurance Portability and Accountability Act (HIPAA) data is stolen, the agency can incur large penalties, up to $1.5 million.

Cause

DBHDS has a decentralized IT governance structure, which led to having 437 disparate sensitive systems it cannot properly manage and maintain. DBHDS lacks the necessary IT resources at the Central Office and facilities to ensure compliance with the requirements in the Security Standard and enterprise security program. Additionally, the current reporting structure is not conducive for coordinating IT efforts between the Central Office and the facilities.

Recommendation

DBHDS should develop a formal plan to consolidate the 437 disparate sensitive systems to a level where the current IT resources can maintain compliance with Security Standard and agency policies, or hire additional resources to do so. DBHDS should evaluate its governance structure to determine the most efficient and productive method to bring the Central Office and the facilities in compliance with the requirements in the Security Standard. DBHDS should also evaluate its IT resource levels to ensure sufficient resources are available to implement any IT governance changes and rectify the control deficiencies. Implementing these recommendations will help ensure the confidentiality, integrity, and availability of DBHDS' sensitive data.

Upgrade Unsupported Technology

Condition

DBHDS does not upgrade information technology applications that are no longer supported by their vendor. The applications using unsupported technology contain sensitive and mission critical data, which increases the risk that a malicious attacker can exploit a known vulnerability. We identified and communicated the control weakness to management in a separate document marked Freedom of Information Act Exempt (FOIAE) under Section 2.2-3705.2 of the Code of Virginia due to it containing descriptions of security mechanisms.

Criteria

The Security Standard, Section SI-2-COV, requires that organizations prohibit the use of products designated as end-of-life/end-of-support by the vendor or publisher.

Consequence

By using end-of-life or end-of-support technology, DBHDS can no longer receive and apply security patches for known vulnerabilities, which increases the risk a malicious attacker will exploit these vulnerabilities leading to a data breach. Additionally, vendors do not offer operational and technical support for end-of-life or end-of-support technology, which affects data availability by increasing the difficulty of restoring system functionality if a technical failure occurs.

Cause

DBHDS is not performing certain tasks to meet the requirements in the Security Standard and has a decentralized IT environment.

Recommendation

DBHDS should dedicate the necessary resources to implement the controls discussed in the communication marked FOIAE in accordance with the Security Standard.

Improve Risk Management Process

Condition

DBHDS does not have a risk management process to support and protect its sensitive systems. We identified and communicated the control weakness to management in a separate document marked Freedom of Information Act Exempt (FOIAE) under Section 2.2-3705.2 of the Code of Virginia due to it containing descriptions of security mechanisms.

Criteria

The Security Standard requires agencies to use specific controls to reduce unnecessary risk to data confidentiality, integrity, and availability in systems processing or storing sensitive information.

Consequence

DBHDS cannot ensure confidentiality, integrity, and availability for its mission critical and sensitive data.

Cause

DBHDS lacks the necessary resources to fulfill the requirements in its enterprise security program and the Security Standard and is not performing certain tasks to meet the requirements in the Security Standard.

Recommendation

DBHDS should dedicate the necessary resources to implement the controls discussed in the communication marked FOIAE in accordance with the Security Standard.

Develop Vulnerability Assessment Process

Condition

DBHDS does not have formal policies or procedures to perform vulnerability assessments on publicly facing and sensitive systems. Additionally, DBHDS is not utilizing vulnerability scanning software or periodically reviewing and evaluating additional system vulnerability tools such as the Microsoft Baseline Security Analyzer (MBSA) and the SQL Best Practice Analyzer (SQL BPA) reports. DBHDS has 437 sensitive systems that require vulnerability scans, and some systems are using outdated and unsupported technology. Establishing a formal process to conduct vulnerability assessments will allow DBHDS to focus on remediating and mitigating the greatest risks to their sensitive systems containing sensitive data.

Criteria

The Security Standard, Sections RA-5 and RA-5-COV, requires DBHDS to have vulnerability scanning procedures, and employ vulnerability scanning tools, analyze scan reports and results from security control assessments, and remediate legitimate vulnerabilities within 90 days.

Consequence

By not having a formal vulnerability assessment process that utilizes vulnerability scanning software and vulnerability assessment tools, DBHDS increases the risk malicious users can discover and exploit known vulnerabilities to potentially compromise the system. DBHDS has multiple systems containing HIPAA data and if a data breach occurs, it can result in large monetary penalties, up to $1.5 million.

Cause

DBHDS' enterprise security program does not contain vulnerability assessment procedures to ensure the proper vulnerability scans and assessment are being done. Performing vulnerability scans, evaluating the scan reports, and remediating legitimate vulnerabilities is not feasible for DBHDS's 437 sensitive systems with the current IT resource level. In addition, DBHDS does not have its own vulnerability scanning software and must procure vulnerability assessments through the Virginia Information Technologies Agency (VITA) resulting in a substantial cost to the agency.

Recommendation

DBHDS should develop and implement a vulnerability assessment process that complies with the requirements in the Security Standard. DBHDS should evaluate the current IT resource level and prioritize vulnerability scans for systems containing sensitive data. DBHDS should research procuring a vulnerability scanning software for the Central Office and facilities to reduce the cost of performing vulnerability assessments. Doing this will ensure DBHDS maintains confidentiality, integrity, and availability of their sensitive data.

Develop Baseline Configurations for Information Systems

Condition

DBHDS does not have documented baseline configurations for their sensitive systems' hardware and software requirements. DBHDS has 437 sensitive systems, with some containing HIPAA data, social security numbers, and Personal Health Information (PHI) data.

Criteria

The Security Standard, Sections CM-2 and CM-2-COV, requires DBHDS to perform the following:

- Develop, document, and maintain a current baseline configuration for information systems;
  (Section 8 Configuration Management: CM-2)

- Review and update the baseline configurations on an annual basis, when required due to environmental changes, and during information system component installations and upgrades;
  (Section 8 Configuration Management: CM-2)

- Maintain a baseline configuration for information system development and test environments that is managed separately from the operational baseline configuration;
  (Section 8 Configuration Management: CM-2)

- Apply more restrictive security configurations for sensitive systems, specifically systems containing HIPAA data; and
  (Section 8 Configuration Management: CM-2-COV)

- Modify individual IT system configurations or baseline security configuration standards, as appropriate, to improve their effectiveness based on the results of vulnerability scanning.
  (Section 8 Configuration Management: CM-2-COV)

Consequence

By not having baseline configurations, it increases the risk DBHDS's 437 sensitive systems will not have minimum security requirements to protect HIPPA data, social security numbers, and PHI data from malicious attempts. Baseline security configurations are essential controls in information technology environments to ensure that systems have appropriate configurations and serve as a basis for implementing or changing existing information systems. If a data breach occurs to a system containing HIPAA data, the agency can incur large penalties, up to $1.5 million.

Cause

DBHDS has procedures documenting application security requirements, but the procedures do not contain minimum baseline configurations. The agency also lacks the necessary resources to properly monitor and maintain baseline configurations for their 437 sensitive systems.

Recommendation

DBHDS should establish and document security baseline configurations for their information systems to meet the requirements in the Security Standard. DBHDS should evaluate the resources necessary to ensure the security baseline configurations are, at a minimum, in place on all 437 sensitive systems. Doing this will help ensure the confidentiality, integrity, and availability of the agency's sensitive data.

Improve Information Security Officer Independence and Grant Proper Authority to Regional Information Security Officers

Condition

DBHDS does not position the Information Security Officer (ISO) role in an organizationally independent unit from the Chief Information Officer (CIO). In addition, DBHDS hired Regional Information Security Officers (RISOs) to assist the ISO and provide information security oversight and governance to its 15 facilities; however, the ISO and RISOs lack the necessary authority to enforce the DBHDS' enterprise security program and the Security Standard. Further, there are currently no consequences for the facilities for noncompliance.

Criteria

The Security Standard, Section 2.4.1, recommends that the ISO report directly to the agency head, where practical, and should not report to the CIO. Section 2.5 also states that the ISO is responsible for developing and managing the agency's information security program.

Consequence

Having the ISO role reporting to the CIO may limit effective assessment and necessary recommendations of security controls in the organization due to possible competing priorities that sometimes face the CIO. In addition, without the proper authority, delegated by the Commissioner, the ISO and RISOs cannot force the Central Office and facilities to comply with the DBHDS enterprise security program.

Cause

In establishing its information security officer position within the organization, DBHDS did not fully consider the need for complete independence of the ISO and the Information Security Office.

Recommendation

DBHDS should evaluate the organizational placement of the ISO to eliminate any conflicts of interest in the implementation of its information security program and controls. While it may not be feasible to have the ISO report directly to the Commissioner, DBHDS should consider placing the ISO role in a different organizational unit reporting to another executive-level position. Further, the Commissioner should give the ISO and RISOs the necessary authority to monitor and regulate compliance with the DBHDS enterprise security program and Security Standard.

Improve Database Security – REPEAT

Condition

DBHDS continues to operate its databases that store its financial activity without implementing the minimum controls in accordance with internal policy, the Security Standard, and industry best practices. We communicated 13 areas of weakness during the fiscal year 2014 audit in detail to management in a separate document marked Freedom of Information Act Exempt (FOIAE) under Section 2.2-3705.2 of the Code of Virginia, due to their sensitivity and description of security controls. Although these weaknesses are still not resolved, we recognize that DBHDS has made progress toward resolving these weaknesses in accordance with their corrective action plan and plans on having these control weaknesses remediated by December 2015.

Criteria

The Security Standard requires implementing specific controls to reduce unnecessary risk to data confidentiality, integrity, and availability.

Consequence

Operating an unsupported and improperly configured database increases the risk of a data breach through an attack that exploits known vulnerabilities in a misconfigured system.

Cause

Management's corrective action plans were to complete and remediate the control weaknesses by October 2015, but the process has taken longer than expected and created a two-month delay. We will continue to provide updates on this finding in future reports until management can fully implement their corrective actions, and we have evaluated them for effectiveness.

Recommendation

DBHDS has made progress toward completing corrective actions and resolving the control weaknesses in accordance with their corrective action plan; therefore, DBHDS should continue to dedicate the necessary resources to completely address the control weaknesses to ensure its procedures are in accordance with the current Security Standard and industry best practices, such as those published by the Center for Internet Security.

Improve IDOLS Security – REPEAT

Condition

DBHDS does not implement certain controls in its Intellectual Disability On-Line System (IDOLS) that contains protected health information. We identified and communicated two inadequate systems security controls to management in a separate document marked Freedom of Information Act Exempt under Section 2.2-3705.2 of the Code of Virginia due to it containing descriptions of security mechanisms.

Criteria

The Security Standard requires implementing specific controls to reduce unnecessary risk to data confidentiality, integrity, and availability.

Consequence

DBHDS increases the risk it will not meet the standards for confidentiality, integrity, or availability by not implementing the necessary controls for IDOLS.

Cause

DBHDS does not manage or establish appropriate information security controls for IDOLS as management does not define its expectations through formal policies and procedures to appropriately configure IDOLS.

Recommendation

DBHDS should dedicate the necessary resources to implement the controls discussed in the communication marked FOIAE in accordance with the Security Standard.

Increase Oversight over Third-Party Providers

Condition

DBHDS is not gaining assurance that their third-party providers have secure IT environments to protect sensitive Commonwealth data. The Security Standard considers third-party providers to be organizations that perform outsourced business tasks or functions on behalf of the Commonwealth. DBHDS has outsourced several of its mission critical business functions including its Electronic Health Records System, which includes Commonwealth and HIPAA data relating to patients served by DBHDS.

Criteria

Section 1.1 of the Security Standard recognizes that agencies may procure IT equipment, systems, and services covered by the Security Standard from third-party providers. In these situations, the Security Standard requires agencies enforce the requirements outlined in the Security Standard through documented agreements with providers and oversight of the services performed.

Consequence

By not having a process to gain assurance over third-party service providers' IT environments, DBHDS cannot validate the providers have effective IT controls to protect its sensitive data.

Cause

DBHDS has not been gaining assurance of its third-party providers IT environments because there is no formal process in its information security program for identifying third-party service providers and providing appropriate oversight.

Recommendation

DBHDS should develop a formal process to gain assurance that its third party providers have secure IT environments to protect sensitive data. One way to do this is by requesting and reviewing Service Organization Control reports. After DBHDS develops a formal process, it should incorporate the process into its information security program.

Develop and Submit an Information Technology Audit Plan - REPEAT

Condition

DBHDS does not coordinate and plan audits over sensitive IT systems to ensure it sufficiently protects data. DBHDS' Internal Audit Department submitted a plan to VITA in December 2014, but had not submitted one the previous five years. The plan submitted in December 2014 included all of DBHDS' 437 sensitive systems; however, VITA rejected the plan because DBHDS did not include each individual sensitive system in the Commonwealth Enterprise Technology Repository (CETR). DBHDS has now input all 437 sensitive systems into CETR and the Internal Audit Department will submit another plan to VITA. In addition, DBHDS does not have an IT auditor to perform the information security audits once VITA approves the plan.

Criteria

The Security Standard, SEC 502-02.2, Section 2.1, requires that agencies submit an IT audit plan to the Chief Information Security Officer (CISO) of the Commonwealth of Virginia on an annual basis. SEC 502-02.2, Sections 1.4 and 2.1, further require Commonwealth agencies to annually update and create a three-year IT audit plan that covers the organization's sensitive IT systems. SEC

502-02.2, Sections 2 and 1.2.5, require IT security audits be conducted by personnel or organizations defined as IT security auditors that have the experience and expertise to perform IT security audits. Additionally, the Security Standard requires that these audits be performed in accordance with either Generally Accepted Government Auditing Standards or International Standards for the Professional Practice of Internal Auditing (IIA Standards). SEC 502-02 further requires in Section 2.2 that IT security audits be performed based on the minimum controls established in the Security Standard, SEC 501.

Consequence

IT security audits determine if reasonable controls are in place to protect sensitive data for each respective system. As DBHDS does not have a schedule to audit each sensitive IT system, DBHDS increases the risk of an IT system being overlooked that may contain significant risks that require remediation. These risks increase the risk of a potential data breach at DBHDS.

Cause

DBHDS Internal Audit did not establish an appropriate IT audit plan due to limited communication with management and a lack of understanding of the SEC 502 requirements. DBHDS Internal Audit also continues to lack an IT audit plan because VITA rejected the plan submitted in December 2014. DBHDS submitted a budget request to hire an IT auditor, but will not know if the request is approved until the General Assembly and Governor approve the next biennial budget.

Recommendation

DBHDS should submit an IT audit plan to VITA and submit timely annual three-year IT audit plans to the Commonwealth's CISO. In addition, DBHDS should hire an IT auditor with the experience and expertise to complete the audit plan or evaluate hiring a private firm if the General Assembly denies the budget request.

Improve Internal Controls over Systems Access - REPEAT

Condition

The Central Office and individual facilities within DBHDS do not have adequate controls in place to ensure system access is appropriate in Kronos (HR and Payroll System), Financial Management System (FMS), Lease Accounting System (LAS), and Fixed Assets Accounting System (FAACS). Specifically:

- Two out of four systems at eight facilities and the Central Office had missing and inaccurate User Access Forms for employee access;

- Two out of four systems at two facilities had employees whose access was not removed timely;

- Two out of four systems at the Central Office had employees with access to a system that was not consistent with their job responsibilities; and

- One out of four systems at one facility had four staff within the Fiscal Division with super user access even though some of the individuals were not providing ongoing administrative duties for the system.

Criteria

The Security Standard, Section AC-2- COV, 2.e-h, requires the prompt removal of system access for terminated or transferred employees. The Security Standard, Section AC-2- COV, 2 i, requires granting access to the system based on a valid access authorization. The Security Standard, Section AC-6, requires agencies to employ the principle of least privilege allowing only authorized access for users, which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

Consequence

Missing and inaccurate forms, untimely removal, inaccurate entry of system access based on completed forms, and access that is not necessary for job responsibilities increases the risk of unauthorized individuals inappropriately entering or approving transactions and could affect the integrity of DBHDS transactions in the system.

Cause

DBHDS does not have adequate policies and procedures over granting, changing, and terminating system access. Specifically, policies and procedures lack the guidance on timeframes and contacts for removal of access as well as what access signifies super user access and how to grant it. In addition, DBHDS has not adequately trained Regional FMS Security Officers to properly grant and change system access.

Recommendation

While management has made progress in these areas within the last year, management should continue to develop, implement, and communicate policies and procedures over granting, changing, and terminating access for all systems at all DBHDS facilities and the central office. In addition, management should properly train Regional FMS Security Officers on the processes surrounding granting and changing system access.

Why the APA Works with DBHDS Internal Audit to Audit Payroll

DBHDS employs over 10,000 salaried and wage employees across 16 facilities. Because of the sizeable nature of this expense to the Commonwealth, DBHDS management must take necessary precautions to ensure the integrity of payments to employees. To determine if controls over payroll were adequate, DBHDS Internal Audit compared the practices of DBHDS to those required by the Commonwealth Accounting Policies and Procedures (CAPP) Manual, resulting in the finding below.

Improve Controls over Payroll

Condition

Individual facilities within the DBHDS do not have adequate controls in place to ensure Human Resources forms are completed and payroll is appropriate. Specifically:

- 45 percent (37 out of 82) of the population tested at three out of four facilities tested did not have proper approval on payroll forms and pay changes;
- 23 percent (nine out of 43) of the population tested at two out of four facilities tested did not have completed employee work profiles, payroll forms, and pay changes; and
- For one facility, fiscal does not review and approve pay action forms and pay action worksheets that are completed for employee pay increases.

Criteria

CAPP Manual Topic 50505, Time and Attendance, states that agencies must verify that all source documents such as timecards, timesheets, or any other authorization used to pay or adjust an employee's pay have been properly completed, authorized by the appropriate party, and entered accurately into CIPPS.

Consequence

Not having proper approval of payroll forms and pay changes increases the risk that DBHDS could pay unauthorized and incorrect salaries.

Cause

These exceptions occurred because the individual facilities either do not have adequate policies and procedures for payroll forms or did not comply with established CAPP Manual guidance or local policies and procedures for payroll forms.

Recommendation

Management across all facilities, not just those tested, should evaluate and update policies and procedures to provide adequate guidance to ensure proper approval and completion of employee work profiles, payroll forms, and pay changes. In addition, human resource and payroll personnel across all facilities should ensure that they receive properly approved and completed employee work profiles, payroll forms, and pay changes before processing these changes.

Why the APA Audits Controls over the *my*VRS Navigator System

The Virginia Retirement System (VRS) has modernized the methods of collecting and reporting creditable compensation, service credit, and contributions for all participating employees. The implementation of the *my*VRS Navigator system shifted the responsibility of updating these records from VRS to the employers, to include DBHDS. Because the records in *my*VRS Navigator are used to calculate total pension liabilities for the Commonwealth, DBHDS management must take all necessary precautions to ensure the integrity of these records. To determine if adequate precautions were taken, we compared the practices of DBHDS to the guidance provided by the Department of Accounts (Accounts) over the VRS billing process.

Improve Controls over the *my*VRS Navigator System – REPEAT

Condition

Individual facilities within DBHDS do not have adequate controls in place to ensure that retirement information for employees is accurate and system access is appropriate. Specifically:

- Seven of nine facilities tested did not confirm contribution snapshots timely;
- Eight of nine facilities tested did not have adequately documented policies and procedures to reconcile their payroll and human resource systems to VRS's *my*VRS Navigator system;
- One of six facilities tested had an individual with inappropriate duplicate *my*VRS Navigator access; and
- Two of nine facilities tested did not properly reconcile payroll, human resources, and *my*VRS Navigator.

Criteria

Accounts Payroll Bulletin Volume 2013-02 states that agencies must certify the contributions snapshot by the tenth of the following month, as it becomes the official basis for VRS billing amounts once certified. In addition, it is best practice to create and document formal policies and procedures to ensure that reconciliations are performed between *my*VRS Navigator and the systems of record for payroll and human resources and to ensure that *my*VRS Navigator system access is both role-based and centered on least privileges.

Consequence

Untimely certification at the agency level impacts the ability of Accounts to process inter-agency transfers for any differences between the amounts confirmed in *my*VRS Navigator and the

retirement contributions actually withheld and paid for all agencies across the Commonwealth. Inadequate written policies and procedures at DBHDS facilities provides insufficient guidance for employees to perform the reconciliations necessary to perform these certifications. Inappropriate access to the *my*VRS Navigator system, through inappropriate duplicate access privileges, creates the potential for inaccurate information to appear in the VRS system data that ultimately determines pension liability calculations for the entire Commonwealth. The VRS actuary uses the information in *my*VRS Navigator to calculate the Commonwealth's pension liabilities and inaccurate data could lead to a misstatement in the Commonwealth's CAFR.

Cause

Staffing shortages, including a lack of cross-training, competing priorities, issues that required research, and inadequate oversight of this process at the local level contributed to the lack of timely certifications at all seven locations. The inappropriate duplicate access observed involved one employee whose access had been entered twice. The facility removed the duplicate access once we identified it.

Recommendation

Management should implement adequate controls and procedures at the facilities that consider staffing and other priorities to ensure timely confirmation of the monthly contribution snapshot. Management should also formally document policies and procedures necessary to perform the monthly reconciliations between the payroll, human resource, and *my*VRS Navigator systems at all facilities. Finally, management should ensure appropriate *my*VRS Navigator system access at all facilities.

Why the APA Audits Hours Worked by Wage Employees

DBHDS employs a significant number of wage employees who are not eligible to participate in the state health insurance plan. Because of the financial penalties associated with violating Federal laws pertaining to health insurance coverage, DBHDS management must take necessary precautions to prevent employees from exceeding allowable hours worked thresholds. To determine if the threshold was exceeded, we compared the hours worked by DBHDS wage employees to the hours allowed by the Virginia Acts of Assembly.

Comply with Hour Restrictions for Wage Employees

Condition

Central Virginia (Central Virginia) and Southwestern Virginia (Southwestern Virginia) Training Centers did not comply with the requirement to prevent wage employees from working more than 1,508 hours. One wage employee at each facility exceeded the allowable hours worked threshold for wage employees during the standard measurement period of May 1, 2014, through April 30, 2015. The employee at Central Virginia worked 1,510.7 hours and the employee at Southwestern Virginia worked 1,526.4 hours. Wage employees are not eligible to participate in the state health insurance plan.

Criteria

Chapter 665 §4-7.01 g. of the 2015 Virginia Acts of Assembly states that "State employees in the legislative, judicial, and executive branches of government, the independent agencies of the Commonwealth, or an agency administering their own health plan, who are not eligible for benefits under the health care plan established and administered by the Department of Human Resource Management ("DHRM") pursuant to Va. Code § 2.2-2818, may not work more than 29 hours per week on average over a twelve month period." DHRM guidance for determining compliance with this requirement defines the Standard Measurement Period as May 1, 2014, through April 30, 2015.

Consequence

Failure to comply with Chapter 665 of the 2015 Virginia Acts of Assembly subjects DBHDS to potential financial penalties for violation of the Federal Affordable Health Care Act by allowing workers to work over the threshold and not receive healthcare benefits.

Cause

A breakdown in monitoring processes at Central Virginia and Southwestern Virginia Training Centers resulted in two wage employees exceeding the allowable hours worked threshold.

Specifically, Central Virginia had turnover in the position responsible for the monitoring. Southwestern Virginia improperly updated KRONOS during implementation in September 2014 and did not enter employee's time from July 2014 through the implementation date into KRONOS; therefore, the system did not properly calculate the hours worked to be compared to the 1,508 requirement.

Recommendation

Management should comply with Chapter 665 §4-7.01 g. of the 2015 Virginia Acts of Assembly and ensure wage employees do not exceed the allowable hours worked threshold of 1,508. This should include identifying employees that could potentially exceed the threshold as they approach the threshold rather than after exceeding it.

Why the APA Audits Fixed Assets Management

DBHDS has 16 individual locations throughout the Commonwealth. As part of its plan to comply with the Department of Justice settlement, DBHDS plans to close three facilities by the end of fiscal year 2020. Because of the large number of fixed assets associated with multiple locations, DBHDS management must take necessary precautions to account for all fixed assets properly. To determine if fixed assets are accounted for properly, we compared the practices of DBHDS to those required by the CAPP Manual.

Improve Policies and Procedures over Fixed Assets – REPEAT

Condition

DBHDS lacks adequately documented and approved policies and procedures for fixed assets. The areas that were not clearly documented and approved include but are not limited to:

- Fixed Assets Accounting and Control System (FAACS)
- Physical inventory
- Additions
- Disposals
- Donations
- Reconciliations
- Intangible assets
- Capital outlay
- Sales and surplus of land and buildings
- Useful life assessment and reevaluation

In addition, multiple DBHDS facilities and Central Office have documented policies and procedures that management has not reviewed since implementation in 2009.

Criteria

CAPP Manual Topic 20905, CARS Reconciliation Requirements, states that CAPP Manual procedures alone never eliminate the need and requirement for each agency to publish its own internal policies and procedures documents, approved in writing by agency management. The lack of complete and up-to-date internal policies and procedures (customized to reflect the agency's staffing, organization, and operating procedures) reflects inadequate internal controls.

Consequence

The lack of fixed assets policies and procedures increases the risk of inaccurate accounting of fixed assets and contributed to the issues discussed in the findings "Improve Controls over Physical Inventory," "Improve Controls over Intangible Assets," and "Improve Controls over Sale of Land."

Cause

DBHDS has not allocated or prioritized the appropriate resources to ensure that such internal policies and procedures over fixed assets are present at all DBHDS facilities and Central Office.

Recommendation

Management should continue to create, communicate, and implement policies and procedures over fixed assets at all DBHDS facilities and the central office. In addition, management should periodically review the policies and procedures to determine whether the policies and procedures need to be updated as a result of changes in agency systems or other processes.

Improve Controls over Physical Inventory

Condition

Individual facilities within DBHDS do not have adequate controls in place to ensure physical inventory is properly performed, documented, and recorded in the Fixed Asset Accounting and Control System (FAACS). In addition, DBHDS facilities do not have adequate processes in place to ensure the facilities properly dispose of capital assets within FAACS and maintain adequate supporting documentation for the disposal. Specifically:

- Two out of 15 facilities with fixed assets did not perform a physical inventory within the last two years. At one facility, 646 assets totaling approximately $78 million were not counted. These assets included assets transferred from a closing facility that the receiving facility did not include in their biennial inventory count and land, buildings, and infrastructure assets that were not inventoried.
- Three out of three facilities tested for adjustments resulting from inventories did not record the removal of nine assets from FAACS timely. Two assets disposed in December 2013 remained in FAACS until November 2014, one asset disposed in July 2014 remained in FAACS until June 2015, and one asset was a patient-owned asset that never should have been entered into FAACS.
- Twelve out of 23 items disposed were not recorded in the correct fiscal year.
- Seven out of 12 assets sold had the associated revenue improperly recorded within the Financial Management System (FMS).

- Six assets disposed had additional depreciation recorded after their actual disposal date occurred.
- Seven disposals had missing or inadequate information on the disposal forms completed to support their removal from FAACS.

Criteria

CAPP Manual Topic 30505, Physical Inventory, states that a physical inventory of fixed assets is required at least once every two years in order to properly safeguard assets and maintain fiscal accountability. The CAPP Manual further compels DBHDS to enter all asset transactions into FAACS timely. In addition, CAPP Manual Topic 30105 states that when an asset has been disposed, the book value must be removed from the appropriate capital asset general ledger account balances, and that disposals should be recorded in FAACS during the fiscal year in which an asset was actually disposed.

Consequence

Improperly performing or recording physical inventories increases the risk of loss, theft, and inaccurate accounting of fixed assets. Improper recording of fixed assets increases the risk that asset balances and depreciation expense are materially misstated, which can affect the facilities' Medicaid reimbursements and the Commonwealth's CAFR.

Cause

DBHDS facilities are not performing inventories according to the frequency schedule given in the CAPP manual. When Southside Virginia Training Center (SVTC) closed, the receiving facility believed that SVTC had already performed the inventory on those assets and; therefore, the receiving facility did not perform an inventory over those items. In addition, that facility does not verify the continued existence of land, buildings, and infrastructure because it believes the risk of the items changing without finance staff knowing is low. However, during this time of facility closures, this risk has increased and so has the necessity for accurate inventories of all assets. The second facility did not perform their inventory within the required two-year period due to scheduling conflicts.

DBHDS does not have adequate processes to ensure timely recording of disposals in FAACS and revenues in FMS. DBHDS facilities gave various reasons for delays in disposal recording. These include not realizing that the sale of buildings also included the land, not performing inventories on building improvements every two years, not properly tracking surplus items located in the on-site warehouse, having limited staff, and moving locations during closure of SVTC. Improperly recorded revenues resulted from Central Office recording the revenues related to the sale of the asset as it typically would for the lease associated with the asset.

Recommendation

Management should improve, communicate, and implement policies and procedures over fixed asset inventories and disposals at all DBHDS facilities and the central office. These policies and

procedures should ensure timely handling and proper documentation of disposals. These procedures should also consider staffing levels to ensure that the procedures are achievable given available staff. In addition, management should perform a physical inventory at least once every two years and correctly record any changes in FAACS timely. This should include verification of the existence of land, buildings, and infrastructure.

Improve Controls over Intangible Assets

Condition

DBHDS' Fiscal Services does not have adequate policies and procedures to identify and capitalize intangible assets. In addition, DBHDS is lacking controls to ensure it properly identifies, track, record, and report all intangibles to Accounts. As a result, Fiscal Services is improperly recording intangible construction-in-progress (CIP) in FAACS and Accounts Attachment 14.

- Fiscal Services did not record $7,079,075 in CIP additions for the Electronic Health Record system during fiscal year 2014 in FAACS, did not record the amount in FAACS in fiscal year 2015 to correct the issue, and did not record the value of the 2014 additions in the beginning balance for fiscal year 2015 in Attachment 14, understating the asset by $7,079,075 in FAACS and the Attachment.
- Fiscal Services did not record $741,000 in CIP additions for the Data Warehouse project during fiscal year 2014 in FAACS, did not record the amount in FAACS in fiscal year 2015 to correct the issue, and did not record the value of 2014 additions in the beginning balance for fiscal year 2015 in Attachment 14, understating the asset by $741,000.
- For the CIP values related to Electronic Health Records and the Data Warehouse, Fiscal Services did not separate them by asset but rather lumped the value of both systems under Electronic Health Records in Attachment 14.

Criteria

CAPP Manual Topic 30325, Software and Other Intangible Assets, states, "During the development stage, evaluate the expenditures to determine whether capitalization appears appropriate. Record the applicable capitalizable expenditures as Construction in Progress. To ensure appropriate financial control of Construction in Progress, project numbers should be assigned to identify related expenditures." In addition, CAPP Manual 30325 indicates that the assets are to be recorded in a timely manner.

Consequence

Improperly recording intangible CIP in FAACS and Attachment 14 could materially impact the financial reporting of current CIP and future intangible capitalization in the Commonwealth of Virginia's Comprehensive Annual Financial Report.

Cause

Fiscal Services does not have written policies and procedures in place over intangibles that include the responsible party, the method, the timing, and the system DBHDS Central Office plans to use to track and report CIP and capitalizable intangibles. In addition, there is a lack of communication between Fiscal Services and Information Technology related to intangibles. Furthermore, Fiscal Services does not have adequate controls to ensure that DBHDS' FMS, FAACS, and Accounts attachments are accurate and consistent.

Recommendation

Fiscal Services should improve the policies and procedures related to intangibles by developing and implementing detailed policies and procedures that include the responsible party, the method, the timing, and the system DBHDS Central Office plans to use to track and report CIP and capitalizable intangibles. The policies and procedures should also indicate date of effectiveness, approver, and date of annual reviews. In addition, Fiscal Services should implement and document a control to ensure all information recorded and reported in FMS, FAACS, and Accounts attachments are accurate and consistent.

Improve Controls over Sale of Land

Condition

DBHDS does not have policies and procedures related to the sale of land. In addition, it does not have an understanding of the total acreage of land currently owned or originally recorded by individual parcel in FAACS. In coordination with the Department of Real Estate Services within the Department of General Services (General Services), DBHDS has been selling off small pieces of land in connection with the closing of its training centers and as needed for highway right of way. During fiscal year 2015, DBHDS developed a formula to determine how much to remove from FAACS when partial land sales occur. However, not knowing the total acreage of land recorded in FAACS for each parcel of land makes it difficult to determine an accurate amount to remove timely when selling partial pieces of land, which resulted in an overstatement of at least $1 million. In addition, DBHDS did not provide Accounts adequate information in the Attachment 14 for Accounts to determine which asset in FAACS was overstated and by how much. Furthermore, DBHDS fiscal does not confirm the proceeds from the sale of land it receives from General Services with support for the sale price and fees.

Criteria

CAPP Manual Topic 30805, Disposal Management, indicates that at the time the disposal transaction is processed, the book value of the asset is removed from the FAACS financial reporting file, which interfaces into the Commonwealth Accounting and Reporting System (CARS). It is important for assets that are no longer under the control of the agency to be disposed in FAACS to ensure that financial statements containing capital asset information are accurate. Furthermore,

agencies should periodically review the capital asset information contained in FAACS to ensure that assets that are no longer under the control of the agency have been properly disposed in FAACS. In addition, disposals should be recorded in FAACS during the fiscal year in which the change in asset status occurred. Finally, it is best practice to confirm the revenues received from other state agencies are accurate through support of the sale and fees.

Consequence

Not understanding the total acreage of land, untimely disposals, not properly completing the Account's attachment, and not confirming the revenue received resulted in an overstatement of $1 million and potentially could result in a larger, material misstatement of assets in the Commonwealth's CAFR.

Cause

DBHDS does not have written policies and procedures in place over the sale of land that include the responsible party, the method, the timing, and the system DBHDS plans to track the sale of land, record the revenue, and report the disposal. In addition, DBHDS does not have a control in place to periodically review the capital asset information related to land in FAACS to ensure accurate recording.

Recommendation

DBHDS should develop, implement, and document detailed policies and procedures related to the sale of land. The policies and procedures should include the responsible party, the method, the timing, and the system DBHDS plans to use to track the sale of land, record the revenue, and report the disposal. The policies and procedures should also indicate the date of effectiveness, approver, and date of annual reviews. In addition, DBHDS should determine how much land each facility owns due to the multiple facility closures occurring. DBHDS should keep track of all sales, transfers, and donations of land and ensure the appropriate amount is removed from FAACS timely. In addition, DBHDS should confirm the revenue received from the sale of land with support of the sale price and fees related to the sale of land. Finally, DBHDS should properly report FAACS discrepancies to Accounts with detailed information such as the facility affected, asset number, and the amount FAACS is overstated or understated.

Improve Process Surrounding Fixed Asset Additions

Condition

Individual facilities within DBHDS do not have adequate policies and procedures in place to ensure fixed assets are recorded in FAACS timely. Nine out of 15 facilities recorded 93 percent of their fiscal year 2015 fixed asset acquisitions more than 30 days after receipt and acceptance of the asset.

In addition, DBHDS' Central Office Architecture and Engineering Services (Architecture and Engineering), does not provide the facility FAACS coordinators with detailed information to allow them to timely transfer assets from Construction in Progress (CIP) to the proper depreciable capital asset category.

Criteria

CAPP Manual Topic 30205, Acquisition Method, states, "All recordable assets, except constructed assets, should be recorded in FAACS as soon as possible after title passes. Except in unusual circumstances, assets should be posted within 30 days after receipt and acceptance of the asset. Asset acquisitions should be posted to FAACS in the fiscal year the asset was acquired. Similarly, asset disposals should be posted to FAACS in the fiscal year the disposal occurred. For equipment, title is considered to pass at the date the equipment is received. Constructed assets are transferred from the construction in progress account to the related building, infrastructure, or equipment accounts when they become operational. Constructed buildings, for example, are assumed to be operational when an authorization to occupy the building is issued, regardless of whether or not final payments have been made on all the construction contracts."

Consequence

Improper recording of fixed assets increases the risk that asset balances including depreciation expense are materially misstated, which can affect the facilities' Medicaid reimbursements and the Commonwealth's CAFR.

Cause

DBHDS does not have adequate processes to ensure timely recording of asset acquisitions in FAACS. DBHDS facilities gave various reasons for delays in asset recording. These include not recording received assets until in use, not forwarding information to the FAACS coordinator timely, not inspecting equipment timely, purchasing large numbers of assets at the end of the fiscal year, avoiding accessing FAACS multiple times, waiting for Bank of America Visa bill indicating purchase, and scheduling data entry at a convenient time rather than when required. In addition, Architecture and Engineering, in managing CIP, does not gather and communicate to facilities the detailed information needed by FAACS coordinators to timely transfer items out of CIP and record them in the appropriate capital asset categories.

Recommendation

Management should create, communicate, and implement policies and procedures over fixed asset recording at all DBHDS facilities and the central office. Facilities should handle inspection and processing of facility paperwork promptly enough to ensure recording of assets within 30 days of receipt. Facilities should plan to have personnel available to process FAACS entries timely when purchasing a large number of assets at one time. Management should ensure personnel involved with capital assets understand the importance of timely asset recording as it affects both depreciation and asset balances. In addition, Architecture and Engineering should obtain adequate information from contractors and provide this to the facilities' FAACS coordinators to allow timely recording of assets transferred out of CIP.

Why the APA Audits the Block Grants for Prevention and Treatment of Substance Abuse

DBHDS receives federal funds and disburses some of the funds to local community service boards as necessary to administer the prevention and treatment of substance abuse within the Commonwealth. The federal government requires management at DBHDS to monitor the community service boards' compliance with the grant requirements. To determine if DBHDS is properly monitoring subrecipients, we compared the monitoring practices of DBHDS to those required by the federal government.

Issue Management Decisions for Subrecipients

Condition

DBHDS does not issue management decisions for audit findings related to the Community Service Boards that receive federal funds from the Block Grants for Prevention and Treatment of Substance Abuse, CFDA #93.959, and other federal funds.

Criteria

OMB Circular A-133, Subpart D--Federal Agencies and Pass-Through Entities §___.400 (d)(5) requires that for audit findings pertaining to Federal awards, the pass-through entity must issue a management decision on each audit finding within six months after receipt of the subrecipient's audit report. Management decisions are defined as the "evaluation by the Federal awarding agency or pass-through entity of the audit findings and corrective action plan and the issuance of a written decision as to what corrective action is necessary."

Consequence

Non-compliance runs the risk of the federal government withholding grant funds or not awarding federal grants to DBHDS. Non-issuance of management decisions is one of the three criterion, under OMB Circular A-133, Subpart C—Auditees §___.315 Audit findings follow-up (b)(4), that allows a subrecipient to deem the associated audit finding as not warranting further corrective action. Therefore, DBHDS is increasing the risk that the Community Service Boards will not properly address audit findings.

Cause

Management is not issuing written management decisions because management is relying on negative confirmation with the Community Service Boards to imply agreement with the corrective action taken.

Recommendation

Management should develop a process to issue and communicate written management decisions for audit findings relating to federal funds as required by OMB Circular A-133, Subpart D--Federal Agencies and Pass-Through Entities§___.400 (d)(5). Management should be aware that in fiscal year 2016 this requirement will be mandated by Uniform Code §200.331. Therefore, management should ensure compliance with the Code of Federal Regulations §200.331 at that time.

Why the APA Audits Compliance with the Statement of Economic Interest

DBHDS has designated 59 people in a position of trust across the state. The Code of Virginia requires all individuals in a position of trust to submit Statement of Economic Interest Disclosure Forms and complete related training. To determine if DBHDS complies with the Code of Virginia, we compared the practices of DBHDS to those required by the Code of Virginia.

Comply with the Code of Virginia Economic Interest Requirements

Condition

DBHDS did not ensure employees designated to be holding a "position of trust" are submitting the Statement of Economic Interest (SEOI) forms timely, nor completing the required Statement of Economic Interest training every two years. In addition, DBHDS does not maintain a record of training attendance as required.

Criteria

Pursuant to Sections 2.2-3114 and 3128 through 3131, of the Code of Virginia, employees designated to be in a "position of trust" must file a form set forth in Section 2.2-3117 semiannually by December 15 for the preceding six-month period complete through the last day of October and by June 15 for the preceding six-month period complete through the last day of April. Additionally, filers must complete orientation training about the Conflict of Interest Act that will help them recognize potential conflicts of interest. The filers must complete this orientation within two months of hire/appointment and at least once during each consecutive period of two calendar years. The Office of the Attorney General offers and approves the training to instruct agencies within the Commonwealth. The training educates employees on how to recognize and avoid a conflict, or the appearance of a conflict, of interest and the measures to remedy the conflict. DBHDS must keep a record of attendance for five years including the specific attendees, each attendee's job title, and dates of their attendance.

Consequence

DBHDS could be susceptible to conflicts of interest that would impair or appear to impair the objectivity of certain programmatic or fiscal decisions made by employees in positions designated as "position of trust." By not requiring employees to complete the training and keeping record of the attendance for the training, DBHDS may not be able to hold its employees accountable for knowing how to recognize a conflict of interest and how to resolve it.

Cause

The Statement of Economic Interest Coordinator is responsible for maintaining and submitting the list of individuals who are required to file a SOEI form. Although he monitors and tracks submissions, the individuals required to file a SOEI form do not follow the instructions he provides them by the required due date. Management relies solely on the Department of Human Resource Management's (Human Resource) required mandatory trainings listing when determining which trainings employees will attend and when. Human Resource erroneously listed this training as a one-time training per Section 2.2-3128. Relying solely on this erroneous information caused management not to issue agency-wide guidance that communicated the requirements for when employees should complete the SOEI training and that the Coordinator should maintain record of attendance for the training.

Recommendation

DBHDS should ensure all employees in a position of trust complete the required SOEI form timely, ensure filers complete training once within each consecutive period of two calendar years, and maintain a record of such attendance for five years.

Why the APA Audits Information System Security

The Department of Health (Health) collects, manages, and stores significant volumes of personal and financial data within its mission critical systems. Because of the highly sensitive and critical nature of this data, Health's management must take necessary precautions to ensure the integrity and security of the data within its systems. We compared Health's practices to those required by the Commonwealth's Information Security Standard in the areas of database security, web application security, oversight of sensitive systems, and information system access.

Approve Vulnerability Scanning Procedures and Review System Vulnerability Scanning Tools

Condition

Health has not developed formal policies or procedures to perform periodic vulnerability scans on their publicly facing and defined sensitive systems. Health also does not periodically review or evaluate certain reports from system vulnerability and baseline scanning tools. Reports from these tools enable system administrators to evaluate and determine if their systems are in line with recommended vendor security settings and industry best practices. Health has multiple publicly facing and sensitive systems that require periodic vulnerability scans.

Criteria

The Commonwealth's Information Security Standard, SEC 501-09, (Security Standard) Section 1.14 Risk Assessment, RA-5 and RA-5-COV, requires Health to have vulnerability scanning procedures. The Security Standard further requires Health to use vulnerability scanning tools, to analyze scan reports and results from security control assessments, and remediate legitimate vulnerabilities within 90 days.

Consequence

Periodically using vulnerability scanning and system baseline assessment tools provide information on sensitive system configuration such as missing critical patches, inappropriate permission levels, and technical configurations and settings to enhance security and optimization. These results should be used by organizations to better enhance and refine the security controls and configurations for sensitive and internet facing systems, thereby reducing security risks. By not having formal procedures to ensure system owners and administrators perform vulnerability scans and not periodically reviewing vulnerability and baseline scanning tools, Health increases the risk that malicious users can discover and exploit known vulnerabilities to potentially compromise the system.

Cause

Health has a vulnerability scanning policy in draft form but the policy is not implemented throughout the agency, and management has yet to approve it. Additionally, Health relies on the Virginia Information Technologies Agency (VITA) to perform system vulnerability scans and run baseline scanning tools, but Health was not requesting or obtaining them for evaluation on a consistent basis.

Recommendation

Health management should approve and implement the vulnerability scanning policy to ensure all system owners and system administrators perform and remediate legitimate vulnerabilities on a timely basis in accordance with the Security Standard requirements. Health should also develop and implement formal procedures to review and evaluate the baseline scanning tools at a regular and defined frequency. Establishing formal policies and procedures, as well as periodically reviewing and evaluating system vulnerability assessment tools will reduce the risk of inconsistent implementations. These policies and procedures will also enable Health's information technology and security resources to perform vulnerability assessment scanning processes to management's defined expectations.

Improve Information Security Officer Independence

Condition

Health does not position the Information Security Officer (ISO) role in an organizationally independent unit from the Chief Information Officer (CIO).

Criteria

Section 2.4.1 of the Security Standard recommends the ISO report directly to the agency head where practical, and should not report to the CIO.

Consequence

Having the ISO role reporting to the CIO may limit effective assessment and necessary recommendations of security controls in the organization due to possible competing priorities that sometimes face the CIO.

Cause

In establishing its ISO role within the organization, Health did not fully consider the need for full independence of the ISO and the CIO. The information security control weaknesses identified during this year's audit highlight the potential competing priorities of having the ISO report directly to the CIO.

Recommendation

Health should evaluate the organizational placement of the ISO to minimize any conflicts of interest in the implementation of their information security program and controls. While it may not be feasible to have the ISO report directly to the agency head, Health should consider placing the ISO role in a different organizational unit reporting to another executive-level position.

Improve VVESTS Web Application Security

Condition

Health and VITA have not implemented certain security controls for the agency's Virginia Vital Events and Screening Tracking System (VVESTS) web application as required by the Security Standard and recommended by industry best practices. We identified and communicated three inadequate systems security controls to management in a separate document marked Freedom of Information Act Exempt (FOIAE) under Section 2.2-3705.2 of the Code of Virginia due to it containing descriptions of security mechanisms.

Criteria

The Security Standard requires implementing specific controls to reduce unnecessary risk to data confidentiality, integrity, and availability.

Consequence

The identified internal control weaknesses increase the risk that Health will not meet its established systems and data security standards for confidentiality, integrity, or availability for VVESTS.

Cause

There are cost and resource constraints affecting Health and VITA's ability to immediately address the control weaknesses, but Health is currently in the process of evaluating the best course of action to remediate the control weakness for VVESTS.

Recommendation

Health should dedicate the necessary resources and continue working with VITA to implement the controls discussed in the communication marked FOAIE in accordance with the Security Standard.

Improve Access Management for Critical Systems – REPEAT

Condition

Some individual department supervisors are not consistently completing and sending employee separation forms (HR-14 forms) to the Office of Human Resources (OHR) in a timely manner. As a result, Health is not able to consistently remove system access for terminated employees from their internal information systems timely. Health did not delete system access timely for terminated employees with access to several critical information systems as follows:

- Commonwealth Integrated Payroll and Personnel System (CIPPS) leave access was removed between 20 and 58 days late for six employees;
- Go Beyond Well Family System access was removed between 18 and 207 days late for three of four employees;
- WebVision access was removed 186 and 576 days late for two of seven employees; and
- PMIS access was removed four and seven days late for two of seventeen employees.

In addition, new user forms do not match the level of WebVision access requested and approved for three out of 25 employees.

Criteria

The Security Standard requires:

"Notifying account managers…when information system users are terminated, transferred, or information system usage or need-to-know/need-to-share changes." In addition, each agency shall "promptly remove access when no longer required."

Health's internal policies also require that OHR strive to process HR-14 Separation Forms within three business days of the date OHR receives the form.

Consequence

These systems contain sensitive employee, financial, and program participant information. Insufficient access management increases the risk of unauthorized use of the systems by terminated employees, which could result in unauthorized changes and could impair data integrity.

Cause

Health is highly decentralized and OHR is not consistently receiving HR-14 Forms timely from local agency and division supervisors. As a result, OHR cannot forward the termination information to the system owners in a timely manner to ensure access is promptly removed. Currently, when an

employee terminates it is the responsibility of the local agency or division supervisor to advise OHR of the termination. Additionally, staff turnover in OHR also contributed to the problem with CIPPS access.

Recommendation

Health should develop detailed written policies to address the timing and routing of new user forms and the HR-14 forms to ensure that information system access is granted and removed timely. This should include specific procedures to address granting, terminating, and reviewing access. Health should also ensure all pertinent staff are trained in the process, including local agency staff.

Improve Access Management at Local Agencies and Divisions

Condition

Health is not reviewing access to its internal accounting system (F&A) monthly at all local agencies and divisions. Monthly reviews of F&A access are part of Health's internal control to ensure end user access is both necessary and reasonable. These reviews are documented through Health's security portal; however, some local agencies and divisions are not performing this access certification and Health's systems security staff are not performing any follow ups.

Criteria

Health's procedures require that each office and health district certify user account and access information through the security portal. These account certifications must be completed via the Portal Account / Access Certification page no later than the tenth of the following month (i.e., certification of accounts for the month of June are due by July 10).

Consequence

Health is a decentralized agency, which makes periodic access reviews essential to ensure all user access is reasonable and necessary. Insufficient access management increases the risk of unauthorized access to F&A, which could allow for improper transactions and unreasonable access to agency data. F&A is a critical financial reporting system and access to it should be managed accordingly.

Cause

Health has not clearly assigned overall responsibility for F&A access management, so it is unclear whose job it is to ensure accountability of the periodic access reviews.

Recommendation

Health should determine the most effective party to assume overall responsibility for F&A monthly access reviews. Once determined, Health should follow up with all local agencies and division departments when their certifications are not received by the due date.

Why the APA Audits HIV Prevention Activities

The HIV Prevention Activities program provides approximately $9 million annually to assist the Commonwealth in establishing and maintaining an HIV prevention program. The program includes both HIV testing and training and is administered by the local health districts. We reviewed time and effort reporting, allowable costs, procurement, reporting and sub-recipient monitoring.

Record Accurate Time and Effort Reporting

Condition

Division of Disease Prevention employees in the Office of Epidemiology (OEPI) did not accurately record their time and effort reporting. Time and effort reporting determines the amount of personal service costs that are billed to federal grants for reimbursement. Instead of reporting time and effort according to the actual activity of each employee, OEPI employees reported their time, each pay period, according to an estimate that was determined before the activity was performed.

Criteria

According to the Code of Federal Regulations 45 CFR §75.430 Compensation—personal services, costs of compensation are allowable to the extent that they are:

(1) Reasonable for the services rendered and conform to the established written policy of the non-Federal entity consistently applied to both Federal and non-Federal activities.

(2) In compliance with Department of Labor regulations, Fair Labor Standards Act (FLSA) (29 CFR part 516). Records indicating the total number of hours worked each day must support charges for the salaries and wages of nonexempt employees.

Health's internal policies over time and effort states, "Program directors are responsible for advising staff of the appropriate time and effort codes to be used for their activities. Time shall be reported based on where the effort is applied and not necessarily where the employee is paid."

Consequence

OEPI's time and effort documentation does not meet federal requirements or Health's internal policies for supporting charges to the HIV Prevention grant. This could lead to costs being disallowed by the grantor, leaving the Commonwealth responsible for the bill.

Cause

OEPI administrative staff did not properly train program employees on federal time and effort reporting requirements. Employees, including the program manager in OEPI, improperly reported and subsequently approved time and effort that was not an after the fact distribution of the actual activity of each employee.

Recommendation

OEPI should ensure all employees, who are split-funded under different revenue sources, are trained on how to accurately record time and effort under federal regulations. Additionally, supervisors reviewing timesheets should have knowledge of hours worked by employees to ensure actual hours worked agree to time reported.

Why the APA Audits Inventory

Health's inventory is material to the Commonwealth's CAFR. Incorrect reporting of inventory could cause material misstatement of total inventories held by the Commonwealth. We reviewed the Inventory Attachment submitted by Health to the Department of Accounts (Accounts), observed year-end inventory counts performed by Health's Central Pharmacy, and performed test counts and recalculations of inventory totals.

Improve Controls over Inventory Reporting

Condition

Health overstated the year-end general government inventory on-hand amount reported to Accounts by $1,017,000. Additionally, Health overstated both the "Donated Inventory Received" and the "Donated Inventory Used" amounts reported to Accounts in total by $545,000. Accounts uses this information in preparing the Commonwealth's CAFR.

Criteria

Health is responsible for ensuring the internal controls over inventory are adequate to ensure financial information reported to Accounts is accurate and fairly stated.

Consequence

The inventory balances reported by Health are reported in the Commonwealth's CAFR. Therefore, misstated amounts by Health could lead to misstatements in the CAFR. In addition, Health was required to resubmit the inventory attachment to correct the errors, resulting in inefficiencies.

Cause

The Pharmacy Director compiles the amounts for inventory on hand based on information from the Cardinal Health inventory management system and physical inventory counts. The Pharmacy Director incorrectly included expired inventory, which is not considered inventory for reporting purposes. The inventory information was forwarded to the Administrative Deputy who did not detect the error, resulting in an overstatement in the inventory reported to Accounts.

The error in donated inventory was due to the Division of Immunization providing incorrect amounts of donated inventory received and used to the Office of Financial Management. This occurred because they did not follow their internal procedures and used the wrong column of data on their year-end worksheet.

Recommendation

The Pharmacy Director and Division of Immunization should follow Health's internal policies and procedures to ensure accurate inventory information is reported in the Commonwealth's CAFR. Additionally, Health should ensure the Administrative Deputy has the ability to determine the precision of the numbers provided by the Pharmacy Director.

Why the APA Audits Access Management for the Medicaid Management Information System

The Medicaid Management Information System (MMIS) stores protected health information for nearly one million individuals and it is used to process approximately $8 billion in medical claims annually. While MMIS is operated by a contractor, the Department of Medical Assistance Services (Medical Assistance Services) is the system owner and they are responsible for ensuring that MMIS is managed in accordance with the Commonwealth's Information Security Standard (Security Standard). To evaluate Medical Assistance Services' management of access for MMIS, we compared internal practices to those required by the Security Standard.

Create Formal Documentation that Facilitates Controlling Privileges in the Medicaid Management Information System – REPEAT

Condition

Medical Assistance Services does not maintain detailed and accurate documentation of each employee's privileges in MMIS. Additionally, Medical Assistance Services has not developed a conflict matrix, documenting the combinations of privileges that create internal control weaknesses.

Criteria

Security Standard, SEC 501-09, AC-1 Access Control Policy and Procedures, requires agencies to develop, disseminate, and review/update annually, formal documented procedures to facilitate the implementation of the access control policy and associated access controls. Additionally, SEC 501-09, Sections 8.1 AC-2(c) and (d), require that agencies establish conditions for group membership and specify access privileges.

Consequence

Without documenting MMIS' privileges and conflicting privileges, Medical Assistance Services is unable to provide system owners and managers with a listing of users and associated privileges that should be used to evaluate the reasonableness of employee access. As a result, management is increasing its risk of granting employees access they do not need, that could violate the concept of separation of duties and create internal control weaknesses.

Cause

Medical Assistance Services' prior year corrective action plan estimated that the agency would develop an automated process to document MMIS privileges by December 31, 2015. However, following the development of this initial correction plan, the agency instead determined that the process would not be implemented until 2018, once a new security system was selected for

MMIS. The delay was to avoid using resources on a security system that will be discontinued. The agency has since altered this plan and now intends on procuring a new Identity Management System in 2016, which will help develop the needed automatic process to document MMIS privileges. Meanwhile in July 2015, the agency began manually reviewing and updating documented privileges with an estimated completion date of February 2016.

Recommendation

Medical Assistance Services should continue working towards properly documenting and evaluating MMIS Access by:

- Documenting privileges and conflicts in MMIS and providing a listing of users and these privileges to system owners and managers;

- Developing an automated process to more efficiently document MMIS privileges and provide a listing of users and these privileges to system owners and managers;

- Requiring systems owners to provide supervisors and the Information Security Officer documentation that facilitates them in evaluating current access and future requests; and

- Requiring systems owners to train supervisors on the different privileges they are allowed to request.

Why the APA Audits Financial System Application Access

Medical Assistance Services, an $8 billion agency, utilizes an internal financial system that is the agency's system of record for financial activity. Financial information in the agency's internal system impacts the financial information reported in the Commonwealth Accounting and Reporting System (CARS). CARS is the financial system that the Department of Accounts uses to report the Commonwealth's financial activity. Because both the internal financial system and CARS are critical to financial reporting to the Commonwealth, management at Medical Assistance Services must properly control access to ensure the integrity of the data within these systems. To evaluate Medical Assistance Services' management of access for its financial system and CARS, we compared internal practices to those required by the Security Standard.

Develop Oracle Conflict Matrix – REPEAT

Condition

Medical Assistance Services has recently documented conflicting modules or responsibilities within Oracle; however, Medical Assistance Services has not yet used the conflict matrix to evaluate segregation of duties controls.

Criteria

Security Standard, SEC 501-08, Section 8.1 AC-2(b) and (c), requires that agencies specify access privileges and establish conditions for group membership.

Consequence

Without documenting modules and roles that conflict, and providing that documentation to the managers requesting and reviewing access, Medical Assistance Services risks granting access that could create a segregation of duties issue. Until conflict matrixes are fully implemented there is still a weakness in internal controls that threatens the integrity of the Commonwealth's financial records, because Oracle interfaces directly with CARS, the Commonwealth's official financial record.

Cause

As of June 30, 2015, Medical Assistance Services had not contributed the necessary resources to document the conflicts. In doing so, the agency did not meet its estimated completion date in its corrective action plan to last year's finding. This plan was in response to our recommendation for management to document the conflicts, including implementing a policy to document the conflicts. Medical Assistance Services instead continued to use their general knowledge of Oracle roles when requesting and reviewing access. Following audit testwork, management provided the conflict

matrix that was subsequently developed on September 4, 2015. This matrix can be used to assess conflicts in future access evaluations.

Recommendation

Medical Assistance Services should continue to incorporate the conflict documentation into its access evaluations in a way that will allow managers to adequately evaluate the reasonableness of each employee's access to ensure proper segregation of duties surrounding fiscal transactions. After management completes their implementation of their new control, we will review its operating effectiveness in future audits.

Limit Access to the 1099 Adjustment and Reporting System

Condition

Medical Assistance Services CARS Security Officer did not remove access to the 1099 Adjustment and Reporting System (ARS), a subsystem of CARS, for individuals which no longer needed access. Seven of thirteen employees we tested retained access to ARS when it was no longer needed to perform their job responsibilities.

Criteria

Security Standard, SEC 501-8, AC-6 and AC-2-COV, states that access should be granted based on the principle of least privilege and be promptly removed when no longer required. Furthermore, the Commonwealth Accounting Policies and Procedures (CAPP) Manual states that an agency's CARS Security Officer is responsible for a comprehensive system of internal controls over CARS tables and files, including ARS.

Consequence

Allowing users to retain ARS access when their job responsibilities no longer require the access increases the risk of unauthorized adjustments to CARS information.

Cause

The Medical Assistance Services Security Officer was unaware that the seven employees had access, as the data obtained from the Department of Accounts (Accounts) for CARS access reviews did not contain the necessary information to properly review ARS access. The data provided by Accounts did not clearly indicate if an employee had ARS access. The column containing information about ARS access was labeled "1099" and was either blank or included the number 2 next to the employee, neither indicator consistently corresponded with an employee having ARS access. Medical Assistance Services did not inquire further as to the meaning of the data or if more detailed data was available. As a result, the agency did not remove access for any of the employees with

either a blank or a two. Without obtaining more detailed data, Medical Assistance Services is unable to identify employees with access.

Recommendation

The CARS Security Officer should confer with Accounts to gain a better understanding of the ARS access information available to Medical Assistance Services, and use this understanding to perform comprehensive reviews of access to ensure that employees do not have unnecessary access to ARS.

Why the APA Audits Security Compliance Audits

Medical Assistance Services uses a number of information systems to administer the Medicaid program. Many of these systems contain sensitive protected health information. While some of the systems used to administer the program are operated by a contractor, Medical Assistance Services is still required to implement policies, procedures, and processes that meet the requirements of the Security Standard and HIPAA. The federal government requires management at Medical Assistance Services to monitor their compliance with these security requirements. The Internal Audit Division of Medical Assistance Services contracts these security compliance reviews to an outside auditor. In the prior year we reviewed the 2013 security compliance audit report issued by Internal Audit. Below we continue to echo their findings and recommendations and encourage Medical Assistance Services to continue to follow its corrective action plans.

Correct Operating Environment and Security Issues Identified by their Security Compliance Audit – REPEAT

Condition

Medical Assistance Services' Internal Audit Division's review, dated January 31, 2014, found 15 exceptions in which the agency did not comply with the VITA Information Security Standard, SEC 501-7.1, and HIPAA security rules. According to management's updated correction plan, dated September 14, 2015, the following four exceptions remain, which they expect to address by the dates listed:

- Risk Assessment Procedures – March 31, 2016
- Logical Access Controls – January 31, 2016
- Training Materials – January 31, 2016
- Policies and Procedures Reviews – January 31, 2016

Criteria

SEC 501-7.1 required that all state agencies develop and implement appropriate policies and procedures that meet the minimum standards outlined within it, to include sub-section 6: Risk Management and sub-section 8: Security Control Catalog.

Consequence

As Medical Assistance Services has not yet corrected previously identified weaknesses, the agency continues to maintain an increased risk to its sensitive information systems and data, with regards to confidentiality, integrity, and availability. Critical information systems and data could be

impacted due to the weaknesses identified above, which would hinder Medical Assistance Services' ability to perform its mission essential functions in support of the Commonwealth.

Cause

As of September 14, 2015, Medical Assistance Services had not contributed the necessary resources to address its information technology security needs and exceptions as reported in the Internal Audit Division's review. In doing so, the agency did not meet its estimated completion date of June 30, 2015, as stated in its original corrective action plan. Internal Audit continues to monitor and test implemented corrective actions and plans to review remaining corrective actions in 2016.

Recommendation

We recommend that Medical Assistance Services continue to follow its updated corrective action plans for the identified weaknesses, which includes developing or acquiring the necessary resources to ensure that appropriate controls are applied over its sensitive information systems and data. In addition, as Medical Assistance Services addresses these weaknesses, the agency should consider the most current Security Standard, SEC 501-09.

Why the APA Audits an Agency's Controls Over their Information in the *my*VRS Navigator System

The *my*VRS Navigator system is used to calculate total pension liabilities for the Commonwealth. Individual agencies, employers, are responsible for updating the records within *my*VRS Navigator related to their employees. As a result, Medical Assistance Services' management must take adequate precautions to ensure the integrity of these records. To determine if management implemented these precautions, we compared the practices of Medical Assistance Services to the guidance provided by the Department of Accounts (Accounts) and the Virginia Retirement System (VRS).

Document *my*VRS Navigator Reconciliations

Condition

Medical Assistance Services' Human Resources Division is not adequately documenting reconciliations between its internal human resources records and VRS' *my*VRS Navigator system, which contains essential retirement data for state employees. Additionally, management has not created policies or procedures detailing who needs to complete which steps to ensure reconciliations, changes, and adjustments for *my*VRS Navigator are performed accurately.

Criteria

The Department of Accounts Payroll Bulletin 2014_05 states that agencies should reconcile the creditable compensation amount in Personnel Management Information System (PMIS) to the creditable compensation amount in *my*VRS Navigator each month when confirming the snapshot. This control ensures that Medical Assistance Services has reviewed and processed all rejected transactions. In addition, the Commonwealth Accounting Policies and Procedures Manual Section 50410 and the VRS Employer Manual over Contribution Confirmation and Payment Scheduling also requires each agency to perform monthly reconciliations. Due to changes in the accounting and reporting standards over pensions, accurate management of compensation and contribution data at the employee level is critical to the Commonwealth's CAFR.

Consequence

The previous salaries for two of the ten Medical Assistance Services employees reviewed with salary changes during the fiscal year were not correctly recorded in *my*VRS Navigator. Without sufficient reconciliation documentation, there is no evidence indicating that Medical Assistance Services identified or addressed these discrepancies.

Cause

Medical Assistance Services' Human Resources Division relies on the instructions from the Commonwealth's Knowledge Center to complete the contribution confirmations. However, the Knowledge Center provides only basic instructions. According to management, the Human Resources Division has not implemented its own policies and procedures over the *my*VRS Navigator reconciliation process because of understaffing and the high volume of daily tasks.

Recommendation

Medical Assistance Services' Human Resources Division should develop *my*VRS Navigator policies and procedures to ensure compliance with *my*VRS Navigator requirements. Additionally, the Human Resources Division should ensure its internal human resources data and *my*VRS Navigator properly reconcile and retain sufficient documentation to demonstrate the identification and correction of reconciling discrepancies.

Why the APA Audits Access Management for the eVA System

In fiscal year 2015, Medical Assistance Services used the eVA System to procure $134 million in goods and services. While the Department of General Services administers eVA, Medical Assistance Services uses the system to control the entire procurement process from requisitioner to supplier and back. As a result, Medical Assistance Services is responsible for ensuring proper access to eVA. To evaluate Medical Assistance Services' management of access for eVA, we compared their internal practices to those required by the eVA Security Standards.

Improve Access Management for the eVA System

Condition

Medical Assistance Services is not ensuring that employees have proper access within the eVA procurement system. Medical Assistance Services did not formally designate its eVA Security Officers nor did it perform 75 percent of the required quarterly access reviews during fiscal year 2015. In addition, two out of 13 employees retained roles that were inappropriate for their job responsibilities.

Criteria

eVA Security Standards require that agencies designate security officers through designation forms, review access on a quarterly basis, and grant employees only the access necessary to perform their assigned job duties.

Consequence

Not properly designating Security Officers can result in unauthorized employees performing security functions for the eVA system. Without formal documentation of designation, management may be limited in their ability to hold employees performing security functions accountable for their actions. Additionally, the lack of regular access reviews contributed to agency employees having roles that were inappropriate for their job responsibilities. Furthermore, due to the lack of properly designated officers, regular reviews, and improper roles, a Security Officer had roles conflicting with their main security role. This conflict could inhibit their ability to impartially monitor agency purchases and approvals as they could potentially overlook their own approval of improper purchases. Finally, another employee had the ability to approve expenditure limits for their supervisor, thereby facing a conflict of interest should they be pressured to make such approvals for their superior.

Cause

Medical Assistance Services was a pilot agency for eVA's initial 2003-2004 implementation, during which time designation forms were not being used. As a result, the agency did not initially designate its Security Officers and did not designate them in the following years in which the forms were required. Reviews were not performed and employees had improper roles as the agency appears to lack an understanding of the Department of General Services' eVA Security Standards and procedures, critical eVA controls, and the access levels offered by its employees' various eVA roles.

Recommendation

Medical Assistance Services should identify its eVA Security Officers through appropriate designation forms and perform the required quarterly access reviews. Security Officers and all other employees should only have access levels appropriate for them to perform their assigned job duties. To achieve this, Medical Assistance Services should allocate appropriate resources and consult with the Department of General Services to gain an understanding of eVA Security Standards and procedures, critical eVA controls, and employee access levels.

Why the APA Audits Information System Security

The Department of Social Services (Social Services) is responsible for managing federally mandated eligibility programs for the Commonwealth of Virginia, such as Temporary Assistance for Needy Families (TANF), Supplemental Nutrition Assistance Program (SNAP), and Child Support Services. In order to manage the significant volume of personal and financial data, Social Services relies on Information Technology systems for the collection, management, and storing of data. Due to the sensitivity of the data, appropriate policies, procedures, and security controls in accordance with the Commonwealth's Information Security Standard (Security Standard), federal regulations, and industry-specific best practices must be in place to ensure its protection from malicious intent and disastrous events.

Expand Change Management Process to Include All IT Environment Production Changes

Condition

Social Services' new change management process does not include all information technology (IT) environment production changes. In July 2015, Social Services started tracking changes to one of its several applications using a centralized change management software.

Criteria

The Security Standard, sections CM-1 and CM-3-COV, require agencies to implement formal change management control policy and procedures.

Consequence

Delaying or not expanding the new change management process to include all IT environment production changes may introduce inconsistent and improper changes to Social Services' IT environment, which may result in unreliable, unavailable or compromised sensitive data.

Cause

Social Services has not yet implemented the formal change process across all IT environment production changes due to the time required to familiarize personnel with the new process and subsequently change behaviors.

Recommendation

Social Services should continue to systematically expand its new change management process to include all IT environment production changes and continue training personnel to facilitate an easy transition and acceptance.

Obtain Assurance of Internal Control Effectiveness from Service Provider Agency

Condition

Social Services does not validate that its service provider, Virginia Information Technologies Agency (VITA), follows agreed-upon internal controls for the application server that executes the rules that determine citizens' eligibility for services.

Criteria

The Commonwealth Accounting Policies and Procedures (CAPP) Manual Topic 10305, Internal Control, requires that a primary agency obtain assurance from a service provider agency that they have adequately assessed their internal control effectiveness.

Consequence

Without validating that VITA has implemented controls to protect the application server that executes the rules that determine citizens' eligibility for services, Social Services risks potential abuse, error or fraud.

Cause

Social Services signed a Memorandum of Understanding (MOU) with VITA for Medicaid Information Technology Architecture (MITA) services. However, the MOU only serves as the agreement governing the relationship between the two agencies and does not provide a current assessment of VITA's internal controls compliance. Additionally, Social Services has not requested and reviewed a Certification of Internal Control from VITA, because Social Services was unaware of the requirement to request a certification.

Recommendation

Social Services should obtain and evaluate a Certification of Internal Control from VITA to verify VITA's assessment of internal controls over the application server that executes eligibility rules. Social Services should subsequently develop a formal process to obtain and review certifications from service provider agencies on an ongoing basis.

Improve Database Security

Condition

Social Services does not secure a sensitive system's supporting database with some minimum security controls required by the Security Standard.

Criteria

We identified essential internal control weaknesses and communicated them to management in a separate document marked Freedom of Information Act Exempt (FOIAE) under Section 2.2-3705.2 of the Code of Virginia, due to it containing descriptions of security mechanisms. The Security Standard requires implementing specific controls to reduce unnecessary risk to data confidentiality, integrity, and availability.

Recommendation

Social Services should dedicate the necessary resources to implement the controls discussed in the communication marked FOIAE in accordance with the Security Standard, and ensure these controls are implemented in a timely manner.

Continue Addressing Weaknesses from the 2014 IRS Safeguard Review

Condition

On April 14, 2014, Social Services received a final report from the U.S. Internal Revenue Service (IRS) regarding the results of a federal safeguard review that took place in November 2013. The testwork conducted was limited to review the safeguards used to protect the confidentiality of federal tax return information, in which multiple significant deficiencies were identified in internal controls and federal compliance.

Criteria

The Internal Revenue Code §6103(p)(4) requires Social Services to meet federal safeguards requirements and implement safeguards to the satisfaction of the IRS to prevent unauthorized access, disclosure, and use of all tax returns and return information, and maintain confidentiality of that information.

Consequence

Non-compliance with federal regulations and safeguards creates a risk for federal tax information, which includes Personally Identifiable Information (PII) and other confidential data, to be compromised by malicious users.

Cause

Social Services has worked VITA during the last several years to develop and implement a Service-Oriented Architecture for eligibility programs used by multiple Commonwealth agencies. As this is an extensive project and is still ongoing in its final waves of implementations, Social Services has lacked the necessary resources to ensure that appropriate safeguards were in place to comply with IRS safeguard requirements.

Recommendation

Social Services should continue to dedicate the necessary resources for resolving the weaknesses identified in the IRS safeguard review, and ensure sensitive federal tax information is protected in accordance with state and federal laws and regulations.

Risk Alert - Upgrade or Decommission End-of-Life Server Operating Systems

The Commonwealth's IT Infrastructure Partnership with Northrop Grumman (Partnership) provides agencies with installation, maintenance, operation, and support of IT infrastructure components, such as servers, desktops, routers, firewalls, and virtual private networks. During our audit we found that the Partnership is not maintaining some of these devices according to the Security Standard, and as a result is exposing the Commonwealth's sensitive data to unnecessary risk.

The Partnership uses end-of-life and unsupported server operating systems in its IT environment that supports mission critical systems for Social Services, Health, and DBHDS. These and other agencies rely on the Partnership to provide current, supported, and updated server operating systems that serve as the foundations for its mission critical and sensitive systems.

The Commonwealth's Information Security Standard, SEC501-09 (Security Standard), Section SI-2-COV, prohibits the use of products designated as "end-of-life" by the vendor. A product that has reached its end-of-life no longer receives critical security updates that rectify known vulnerabilities that can be exploited by malicious parties.

Specifically, the Partnership maintains 12 server operating systems for Social Services, 12 server operating systems for Health, and 67 server operating systems for DBHDS that are officially designated as end-of-life per the vendor. The Partnership's use of unsupported server operating systems increases the risk that existing vulnerabilities will persist in the server operating systems without the potential for patching or mitigation. These unpatched vulnerabilities increase the risk of cyberattack, exploit, and data breach by malicious parties. Additionally, vendors do not offer operational and technical support for server operating systems designated as end-of-life, which increases the difficulty of restoring system functionality if a technical failure occurs.

The agencies are aware of this issue and are working with the Partnership to develop remediation plans to upgrade or decommission the end-of-life server operating systems. Until then, the agencies and the Partnership have installed additional security controls to attempt to reduce some of the risk that the end-of-life server operating systems introduce into the IT Environment.

Social Services, Health, and DBHDS should continue working with the Partnership to upgrade or decommission all of the end-of life server operating systems prior to their remediation plan deadline. Doing this will further reduce the risk to the confidentiality, integrity, and availability of sensitive Commonwealth data and achieve compliance with the Security Standard.

Commonwealth of Virginia

Auditor of Public Accounts

Martha S. Mavredes, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

December 15, 2015

The Honorable Terence R. McAuliffe
Governor of Virginia

The Honorable Robert D. Orrock, Sr.
Vice-Chairman, Joint Legislative Audit
and Review Commission

We have audited the financial records and operations of the **Agencies of the Secretary of Health and Human Resources**, as defined in the Audit Scope and Methodology section below, for the year ended June 30, 2015. 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 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 the Agencies of the Secretary of Health and Human Resources' financial transactions as reported in the Comprehensive Annual Financial Report for the Commonwealth of Virginia for the year ended June 30, 2015, and test compliance for the Statewide Single Audit. In support of this objective, we evaluated the accuracy of recorded financial transactions in the Commonwealth Accounting and Reporting System and in each agency's accounting records, reviewed the adequacy of each agency's internal control, tested for compliance with applicable laws, regulations, contracts, and grant agreements, and reviewed corrective actions of audit findings from prior year reports.

Audit Scope and Methodology

The Agencies of the Secretary of Health and Human Resources' management has responsibility for establishing and maintaining internal control and complying with applicable laws and regulations. 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 significance and risk in determining the nature and extent of our audit procedures. Our review encompassed controls over the following significant cycles, classes of transactions, and account balances at these four agencies:

Department of Behavioral Health and Developmental Services

- Accounts receivables
- Capital outlay
- Fixed asset management
- Federal revenues, expenses, and compliance for:
  - Block Grants for Prevention and Treatment of Substance Abuse
- Operational expenses
- Payroll expenses
- Institutional revenues
- Community Service Board contracts
- Information system security
- Systems access controls
- *my*VRS Navigator

Department of Health

- Accounts receivable
- Federal revenues, expenses, and compliance for:
  - Special Supplemental Nutrition Program for Women, Infants, and Children
  - Child and Adult Care Feeding Program
  - HIV Prevention Activities
  - Hospital Preparedness Program
  - Affordable Care Act (ACA) Maternal, Infant, and Early Childhood Home Visiting Program
- Payroll expenses
- Support for local rescue squads
- Collection of fees for services
- Cooperative agreements between Health and local government, which includes:
  - Aid to local governments
  - Allocation of costs
  - Reimbursement from local governments
- Accounts payable
- Information system security
- *my*VRS Navigator

Department of Medical Assistance Services

Federal revenues, expenses, and compliance for:
- Medicaid program
- Children's Health Insurance Program

Accounts receivable

Accounts payable

Contract management

System access controls

Utilization units

*my*VRS Navigator

Department of Social Services

Federal revenues, expenses, and compliance for:
- Supplemental Nutrition Assistance Program Cluster
- Temporary Assistance for Needy Families Cluster
- Low-Income Home Energy Assistance Program

Eligibility for:
- Medicaid

Budgeting and cost allocation

Network and system security

Child Support Enforcement asset accuracy

Supplemental Nutrition Assistance Program supplemental information

Accounts payable

*my*VRS Navigator

The following agencies under the control of the Secretary of Health and Human Resources are not material to the Comprehensive Annual Financial Report for the Commonwealth of Virginia nor have a federal program that is required to be audited as part of the Statewide Single Audit. As a result, these agencies are not covered by this report:

Department for Aging and Rehabilitative Services
Department for the Blind and Vision Impaired
Department for the Deaf and Hard-of-Hearing
Department of Health Professions
The Office of Children's Services
Virginia Board for People with Disabilities
Virginia Foundation for Healthy Youth

We performed audit tests to determine whether the Agencies of the Secretary of Health and Human Resources' 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; re-performance of automated processes; inspection of documents, records, contracts, reconciliations, and board minutes; and observation of each agency's operations. We tested transactions, system access and performed analytical procedures, including budgetary and trend analyses. Where applicable, we compared an agency's policies to best practices and the Commonwealth's Information Security Standard.

Conclusions

We found that the Agencies of the Secretary of Health and Human Resources, as defined in the Audit Scope and Methodology section above, properly stated, in all material respects, the amounts recorded and reported in the Commonwealth Accounting and Reporting System, each agency's accounting system, and other financial information they reported to the Department of Accounts for inclusion in the Comprehensive Annual Financial Report for the Commonwealth of Virginia. These agencies record their financial transactions on the cash basis of accounting, which is a comprehensive basis of accounting other than accounting principles generally accepted in the United States of America.

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 entitled "Audit Findings and Recommendations."

The Agencies of the Secretary of Health and Human Resources have taken adequate corrective action with respect to audit findings reported in the prior year that are not repeated in this letter.

Exit Conference and Report Distribution

We discussed this report with management at the Agencies of the Secretary of Health and Human Resources as we completed our work on each agency. Management's responses to the findings identified during our audit are included in the section titled "Agency Responses." We did not audit management's responses and, accordingly, we express no opinion on them.

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.

AUDITOR OF PUBLIC ACCOUNTS

GDS/alh

JACK BARBER, M.D.
INTERIM COMMISSIONER

COMMONWEALTH of VIRGINIA

DEPARTMENT OF
BEHAVIORAL HEALTH AND DEVELOPMENTAL SERVICES
Post Office Box 1797
Richmond, Virginia 23218-1797

Telephone (804) 786-3921
Fax (804) 371-6638
www.dbhds.virginia.gov

MEMORANDUM

TO: Ms. Martha Mavredes - Auditor of Public Accounts

FROM: Jack Barber, M.D.

SUBJECT: *Responses to Management Comments - FY 2015 APA Audit*

DATE: January 15, 2016

The purpose of this memo is to provide the Department of Behavioral Health and Developmental Services (DBHDS) responses to management comments issued by the APA as part of the FY 2015 annual audit of the Deprtment. These responses are for inclusion in the Health and Human Resources, FY 2015 audit report.

Management Comment – Improve IT Governance:
The purpose of this memo is to provide the Department of Behavioral Health and Developmental Services (DBHDS) response to the management comment titled – Improve IT Governance. The Department concurs with the audit comment. The Department will do the following to address this issue:

- November 2015, the Department established the Agency IT Advisory Committee (AITAC) whose purpose is to identify enterprise opportunities, establish standards, reduce the number of applications, ensure security compliance, and improve service delivery. This committee reports through the DBHDS CIO, to the Agency IT Strategic Planning Committee (AITSPC) for the purpose of coordinating IT related activities towards those goals. Meetings and conference calls and various IT collaborations are underway.

- December 2015, the Department established the agency-wide Change Management forum that coordinates operational activities to help ensure smooth, secure

implementations. Meetings and conference calls with published action items are underway.

Implementation of the response to this finding was completed as of December 31, 2015. The responsible party for completion of the implementation of this response was Tim Bass, Chief Information Officer.

Management Comment – Upgrade Unsupported Technology:
The purpose of this memo is to provide the Department of Behavioral Health and Developmental Services (DBHDS) response to the management comment titled – Upgrade Unsupported Technology. The Department concurs with the audit comment. The Department will do the following to address this issue:

- The Department continues to make adjustments to its IT governance structure in an effort to achieve modernization and improved security and service levels -- reference implementation of the Agency IT Advisory Committee (AITAC), November 2015, and the Change Management forum, December 2015, discussed in our response to Management Comment #18.

- As of December 2015, the Department has identified 437 applications, largely because of a previous deficit in Enterprise IT collaboration. By June 30, 2016, the office of the Chief Information Officer will publish an Application Modernization Plan (developed in collaboration with the AITAC membership) that will reduce the number of applications from the current level of 437 to 215 by December 31, 2017. The plan will provide reduction milestones for December 31, 2016, June 30, 2017, and December 31, 2017.

Implementation of the response to this finding will be completed by December 31, 2017, specific task dates are noted above. The responsible party for ensuring completion of the implementation of this response is Tim Bass, Chief Information Officer (primary) and AITAC membership (secondary).

Management Comment – Improve Risk Management Process:
The purpose of this memo is to provide the Department of Behavioral Health and Developmental Services (DBHDS) response to the management comment titled – Improve Risk Management Process. The Department concurs with the audit comment. The Department will do the following to address this issue:

- The Department's Information Security (IS) team will review current risk assessments to ensure that they are completed and filed in accordance with SEC501-09 by April 30, 2016.

Implementation of the response to this finding will be completed by April 30, 2016. The responsible parties for ensuring completion of the implementation of this response are Tim Bass,

Chief Information Officer (primary) and Suzanne Battaglia, Acting Chief Information Security Officer (secondary).

Management Comment – Develop Vulnerability Assessment Process:
The purpose of this memo is to provide the Department of Behavioral Health and Developmental Services (DBHDS) response to the management comment titled – Develop Vulnerabiity Assessment Process. The Department concurs with the audit comment. The Department will do the following to address this issue. However, please note that the the Department sought but did not receive funding for the requested vulnerability assessment software or related position and, as a result, will need to mitigate (to the greatest extent possible) this deficit.

- The Department's Information Security (IS) team will consult with two sources – the Agency IT Advisory Committee (AITAC) and the VITA Information Security team – to brainstorm and develop options for gaining access to vulnerability assessment tools that already exist in the Commonwealth and may be available through free trials or limited license extensions. This will also include a review of all existing tools and utilities that may (when combined) offer evidence of vulnerabilities.

- The IS team will develop a specific vulnerability assessment approach and plan (in collaboration with the AITAC) based upon the previous analysis. This plan will also address appropriate system logging, compliant with security related standards.

- The IS team will present this plan to the Chief Information Officer for review, approval and initial implementation by December 31, 2016.

Implementation of the response to this finding will be completed by December 31, 2016. The responsible parties for ensuring completion of the implementation of this response are Tim Bass, Chief Information Officer (primary) and Suzanne Battaglia, Acting Chief Information Security Officer (secondary) and AITAC membership (secondary).

Management Comment – Develop Baseline Configurations for Information Systems:
The purpose of this memo is to provide the Department of Behavioral Health and Developmental Services (DBHDS) response to the management comment titled – Develop Baseline Configuration for Information Systems. The Department concurs with the audit comment. The Department will do the following to address this issue:

- In consultation with the Agency IT Advisory Committee (AITAC), the Department's Business Solutions Development (BSD) and Production Support (PS) teams will draft an outline categorization of the applicable hardware/software standards and types of testing that need detailing.

- The BSD and PS teams will then draft, based upon CO knowledge and experience, the details for each category and (when complete) that draft material will be reviewed and adjusted by the AITAC membership.

- After the AITAC review/modifications, the materials will be presented to the Chief Information Officer for approval and appropriate publication within the Department.

Implementation of the response to this finding will be completed by March 31, 2016. The responsible parties for ensuring completion of the implementation of this response are Tim Bass, Chief Information Officer (primary) and Don Tyson, Business Solutions Development Manager (secondary), John Willinger Production Support Manager (secondary) and AITAC membership (secondary).

Management Comment – Improve Information Security Officer Independence and Grant Proper Authority to Regional Information Security Officers:
The purpose of this memo is to provide the Department of Behavioral Health and Developmental Services (DBHDS) response to the management comment titled - Improve Information Security Officer Independence and Grant Proper Authority to Regional Information Security Officers. The Department does not concur with the audit comment.

- While the ISO reports to the Agency CIO, that reporting structure does not limit effective security assessments or recommendations. The ISO has been given, and will continue to be given, full access to communicate directly with all Department executives, including the Interim Commissioner, and allowed to present objective materials and determinations wherever and whenever needed. The reasons behind the reporting relationship to the CIO involve coordination of service delivery, proper resourcing, project organization, organizational collaboration, and solution design.

If there are questions or comments about this response, please contact Tim Bass or Randy Sherrod.

Management Comment – Improve Database Security:
The purpose of this memo is to provide the Department of Behavioral Health and Developmental Services (DBHDS) response to the management comment titled – Improve Database Security. The Department concurs with the audit comment. The Department will do the following to address this issue:

- The Department has completed all FMS upgrades as of December 25, 2015. The corrected SQL deficiencies in FMS will be verified.

- The Department's Business Solutions Development (BSD), in collaboration with the Department's Production Support (PS) team and the Agency IT Advisory Committee,

will complete a schedule for remediating all hardware and software (according to Commonwealth standards).

Implementation of the response to this finding will be completed by February 1, 2016. The responsible parties for ensuring completion of the implementation of this response are Tim Bass, Chief Information Officer (primary), Don Tyson, Business Solutions Development Manager (secondary), John Willinger, Production Support Manager (secondary), and AITAC membership (secondary).

Management Comment – Improve IDOLS Security:
The purpose of this memo is to provide the Department of Behavioral Health and Developmental Services (DBHDS) response to the management comment titled – Improve IDOLS Security. The Department concurs with the audit comment.

- The Department sought but did not receive funding for the requested log monitoring software or related position and, as a result, will need to mitigate (to the greatest extent possible) this deficit.

- The Department's Information Security (IS) team and Production Support (PS) team will consult with two sources – the Agency IT Advisory Committee (AITAC) and the VITA Information Security team – to brainstorm and develop options for gaining access to log monitoring tools that already exist in the Commonwealth and may be available through free trials or limited license extensions. This will also include a review of all existing tools and utilities that may (when combined) offer monitoring capabilities.

- The IS and PS teams will develop a specific log monitoring approach and plan (in collaboration with the AITAC) based upon the previous analysis.

- The IS and PS teams will present this plan to the Chief Information Officer for review, approval and initial implementation by December 31, 2016

Implementation of the response to this finding will be completed by December 31, 2016. The responsible parties for ensuring completion of the implementation of this response are Tim Bass, Chief Information Officer (primary), Suzanne Battaglia, Acting Chief Information Security Officer (secondary), and AITAC membership (secondary).

Management Comment – Increase Oversight over Third-Party Providers:
The purpose of this memo is to provide the Department of Behavioral Health and Developmental Services (DBHDS) response to the management comment titled - Increase Oversight Over Third-Party Providers. The Department concurs with the audit comment. The Department will do the following to address this issue:

- The Department's Information Security (IS) team will create an accurate (ongoing) list of all third party IT service providers to DBHDS.

- For each relevant Third Party, the appropriate control reports they are obligated to provide by state/federal statute (and by way of established contracts with the Department and/or Commonwealth) will be determined.

- The IS team (through the Chief Information Security Officer) will, for each relevant Third Party, make a recommendation to the Chief Information Officer and as to which report(s) will be most informative and helpful in determining proper security/data controls are in place.

- The Chief Information Officer will review the recommendations, make adjustments and give final approval.

- Once approved, a process will be established within the IS team (through the Chief Information Security Officer) to review and report on the appropriate reports (per relevant Third Party) within 60 days of publication (with "publication" meaning available to the Department).

- Each report will contain a security/data safety assessment as well as any recommended actions for the Department to pursue.

- The Chief Information Officer will review these reports and inform the DBHDS Executive Team of issues and recommended next steps (if any).

Implementation of the response to this finding will be completed by May 30, 2016. The responsible parties for ensuring completion of the implementation of this response are Tim Bass, Chief Information Officer (primary) and Suzanne Battaglia, Acting Chief Information Security Officer (secondary).

Management Comment – Develop and Submit an Information Technology Audit Plan:
The purpose of this memo is to provide the Department of Behavioral Health and Developmental Services (DBHDS) response to the management comment titled - Develop and Submit an Information Technology Audit Plan. The Department concurs with the audit comment. DBHDS is committed to completing all of the requirements of Commonwealth's Information Technology Security Audit Standard, SEC 502-02.2. DBHDS submitted an IT Audit Plan to VITA on November 9, 2015. In addition, the Governor's budget for the 2016-2018 biennium includes funding for additional resources to complete the audits listed in the audit plan. DBHDS has also committed one-time funds to outsource the completion of some sensitive IT systems audits.

Implementation of the response to this audit finding is ongoing. The audit plan was submitted to VITA on November 9, 2015. Once the Governor's budget is approved by the Virginia General Assembly, DBHDS will begin recruiting for an IT auditor. The responsible party for ensuring implementation of the response to this finding is Randy Sherrod.

Management Comment – Improve Internal Controls over Systems Access:
The purpose of this memo is to provide the Department of Behavioral Health and Developmental Services (DBHDS) response to the management comment titled – Improve Internal Controls over Systems Access. The Department concurs with the audit comment. The Department will do the following to address this issue:

- The Department's Information Security (IS) team will (on a bi-monthly basis, thus sixtimes per year) provide a Department-wide security awareness email (in addition to the normal security awareness email campaign) that reminds all management of their responsibility to (1) ensure their staffs' access is supported by accurate and (appropriately) approved security request documentation, and (2) that requests for access must be based on the concept of "least required privilege."

- The IS team will establish a spot-check process whereby (on a bi-monthly basis, thus sixtimes per year) the access privileges for tworandomly selected staff from CO and each of the facilities are reviewed for completeness and accuracy (needed adjustments will be coordinated with management as needed).

- The IS team will establish a process whereby (on a monthly basis) an email will be distributed to all HR departments requesting a list of staff who have resigned, retired or otherwise been terminated for any reason within the past calendar month. Follow-up communications with the appropriate management will immediately occur if action to remove their access privileges has not yet been initiated.

Implementation of the response to this finding will be completed by July 1, 2016. The responsible parties for ensuring completion of the implementation of this response are Tim Bass, Chief Information Officer (primary) and Suzanne Battaglia, Acting Chief Information Security Officer (secondary).

Management Comment – Improve Controls over Payroll:
The purpose of this memo is to provide the Department of Behavioral Health and Developmental Services (DBHDS) response to the management comment titled - Improve Controls Over Payroll. The Department concurs with the audit comments as the payroll testwork was completed by the DBHDS Office of Internal Audit. In addition, the Department has agreed with the responses to the findings that were given by the four facilities where payroll testwork was completed. The responses will satisfy the recommendations made in this finding.

Implementation of the response to this finding will be completed by June 30, 2016. The responsible party for ensuring implementation is Randy Sherrod.

Management Comment – Improve Controls over the myVRS Navigator System:
The purpose of this memo is to provide the Department of Behavioral Health and Developmental Services (DBHDS) response to the management comment titled - Improve Controls over the myVRS Navigator System. The Department concurs with the audit comment. DBHDS will ensure that VNAV snapshot reconciliations are completed in a timely manner. In addition, policies and procedures will be enhanced to adequately describe how the reconciliations of FMS and CIPPS to VNAV are to be completed. DBHDS will also ensure that no employee has duplicate accounts in VNAV by reviewing the access levels in that system.

Enhancements to policies and procedures and the review of access levels in VNAV will be completed by 6/30/2016. The responsible parties for implementation of this response are Stacy Pendleton and Randy Sherrod.

Management Comment – Comply with Hour Restrictions for Wage Employees:
The purpose of this memo is to provide the Department of Behavioral Health and Developmental Services (DBHDS) response to the management comment titled – Comply with Hour Restrictions for Wage Employees. The Department concurs with the compliance finding and will continue to make every effort to ensure that no wage employee exceeds 1,508 hours worked during the time period of May 1st through April 30th. This will be done by continuing to monitor the hours worked by each wage employee. The Department feels that adequate controls are in place to monitor the number of hours worked by these employees as there were only two exceptions found out of a population of more than 700 wage employees.

The implementation of this response will be completed by April 30, 2016. The responsible party for ensuring implementation of this response is Randy Sherrod.

Management Comment – Improve Policies and Procedures over Fixed Assets:
The purpose of this memo is to provide the Department of Behavioral Health and Developmental Services (DBHDS) response to the management comment titled - Improve Policies and Procedures over Fixed Assets. The Department concurs with the audit comment. DBHDS is committed to following all of the requirements of Department of Accounts contained in the Commonwealth Account Policies and Procedures (CAPP) manual. DBHDS will create, if necessary, and update all departmental instructions related to its accounting practices as the new state financial system (CARDINAL) is rolled-out.

Implementation of the response to this finding will be completed by June 30, 2016. The responsible party for ensuring completion of the implementation of this response is Ken Gunn – DBHDS Director of Financial Reporting.

Management Comment – Improve Controls over Physical Inventory:
The purpose of this correspondence is to provide the Department of Behavioral Health and Developmental Services (DBHDS) response to the audit recommendation titled – Improve Controls over Physical Inventory. CAPP manual topic 30505 covers processes attributable to the physical inventory of capital assets while CAPP topic 30105 covers disposal procedures. As a result of this, DBHDS does not view this issue as one of lacking appropriate policies but a lack of proper execution of existing fixed asset policies and the necessity to strengthen existing procedures locally where needed.

DBHDS will continue to abide by the appropriate sections of the CAPP manual published by the Department of Accounts and give appropriate attention to those facilities that are in need of improvement with regard to both procedural development and execution of those procedures.

Implementation of the response to this finding will be completed by June 30, 2016. The responsible party for ensuring completion of the implementation of this response is Ken Gunn – DBHDS Budget Operations and Financial Reporting Director.

Management Comment – Improve Controls over Intangible Assets:
The purpose of this memo is to provide the Department of Behavioral Health and Developmental Services (DBHDS) response to the management comment titled Improve Controls over Intangible Assets. The Department concurs with the audit comment.

The Department appropriately reported to DOA in Attachment 14 during that assessment period, to the best of our knowledge and to the extent of the information available. Once it was realized that CIP for multiple intangible asset projects had been underreported, FAACS was updated accordingly.

During a recent meeting with APA staff, an in-depth discussion on expenses allowed to be recorded under intangible assets raised additional questions on the type of expenses to be recorded. Based on this discussion, the Department is performing another review of all expenses associated with these projects to ensure they meet requirements.

Fiscal Services will develop a written policy over the recording of intangibles. The departmental instruction will provide specific guidance on the tracking and recording of capitalizable intangibles June 30, 2016.

Implementation of the response to this finding will be completed by June 30, 2016. The responsible party for ensuring completion of the implementation of this response is Phil Peter.

Management Comment – Improve Controls over Sale of Land:
The purpose of this memo is to provide the Department of Behavioral Health and Developmental Services (DBHDS) response to the management comment titled - Improve Controls over Sale of Land. The Department concurs with the audit comment.

The Department only manages the properties: The Department of General Services (DGS), Division of Real Estate Services (DRES) sells off various size pieces of land and maintains an inventory of the state owned real estate. The inventory is available to the public at the following website in Acrobat Reader or Microsoft Excel format: (http://dgs.state.va.us/DivisionofRealEstateServices/StateOwnedRealEstate/tabid/1524/Default.aspx)

The Department is in full compliance with DGS and TD regulations, and the Department did provide the Department of Accounts (DOA) the information required in Attachment 14, to the best of its knowledge.

Until recently, the Department had not declared any surplus real estate, and thus there were no policies or procedures in place for such transfers and sales. DRES controls all aspects of easements, transfers and sale of land and works in conjunction with DBHDS to ascertain the amount and value of the land. DRES provides this information to DBHDS at the conclusion of any filing of easement, transfer or sale. DBHDS will develop and implement policies and procedures for updating the facility FAACS based on the information received from DRES. These policies and procedures will include:

1. request from all DBHDS facilities to annually access the DGS/DRES published inventory to reconcile the facility FAACS records to the listed state owned real estate
2. establish a communication flow from DGS/DRES to each agency managing a FAACS inventory of real estate to receive a copy of any official (deed) document making changes to a listed asset,
3. review the FAACS listings for all DBHDS land holdings on an annual basis assuring that the Attachment 14 accurately reports the land assets to the Department of Account.

Please note, as referred to in the attached Department guideline, the transfer of real estate title may take months and the documentation associated is outside of DBHDS' control. There may be a lag time between the property title transfer and receipt of a copy of the deed, the guideline addresses this issue. The same lag time may exist with receipt of the residuals from DGS, via TD, as each agency deducts the costs associated with the property and expenses related to the transaction.

Implementation of the response to this finding will be completed by June 30, 2016. The responsible party for ensuring completion of the implementation of this response is Joe Cronin.

Management Comment – Improve Process Surrounding Fixed Asset Additions:
The purpose of this memo is to provide the Department of Behavioral Health and Developmental Services (DBHDS) response to the management comment titled Improve Process Surrounding Fixed Asset Additions. The Department concurs with the audit comments. A departmental instruction will be developed and placed in effect by July 1, 2016, in order to standardize

expectations on the handling of Fixed Asset addition and to stipulate the process by which each facility complies with regulations.

Implementation of the response to this finding will be completed by July 1, 2016. The responsible party for ensuring completion of the implementation of this response is Ken Gunn – DBHDS Director of Financial Reporting.

Management Comment – Issue Management Decisions for Subrecipients:
The purpose of this memo is to provide the Department of Behavioral Health and Developmental Services (DBHDS) response to the management comment titled – Issue Management Decisions for Subrecipients. The Department concurs with the audit comment and will continue to strive to meet all Office of Management and Budget A-133 Sub-Recipient Monitoring requirements. This includes continuing to monitor the external audit reports of the CSBs, monitoring the Federal Clearing House, and notifying the CSBs that have findings related to federal funds to ensure proper corrective actions are being taken.

This finding related to one community services board (CSB) - Planning District One - located in Big Stone Gap, Virginia. The internal control finding was a lack of appropriate separation of duties due to limited staff performing accounting responsibilities at the CSB. The CSB submitted a plan of corrective action December 1, 2014 that was acceptable to DBHDS. The plan outlined compensating controls to offset the effect of the lack of separation of duties. These included requirements that the contract agency to which the CSB passes funding (both state and Federal) reconcile amounts that it receives with amounts received by the CSB; two signatures are required for all checks; Executive Director review of all checks and purchase orders prior to payment, and, routine review of financial reports and budgets by the CSB Board of Directors.

Currently, the DBHDS sub-recipient monitoring process consists of the following procedures:

1. Each CSB Single Audit is reviewed by the Office of Budget and Financial Reporting. This review consists of financial analysis of GAAP basis financial statements; independent auditors reports on compliance for each Major Federal program, internal controls over financial reporting, an analysis of findings of compliance or deficiency in internal control and a review of the plan of corrective action applicable to audit findings in the report.

2. The review concludes with an assignment of risk to each CSB based upon the results of the above procedures.

3. The highest risks are assigned to those CSBs that have compliance issues or significant deficiencies related to internal controls.

4. Once the risk assessment is completed, a summary report is presented to the Office of Internal Audit.

5. The Office of Budget and Financial Reporting, Office of Internal Audit, and our program offices meet to discuss the risk assessments and to determine which CSBs will receive a field site review during the coming year. The Office of Internal Audit performs five field site reviews per year and follows up on previous filed site reviews as necessary. A field site review of Planning District One CSB was performed in June 2015. The lack of segregation of duties was reviewed along with an assessment of compensating controls outlined in the CSB's Corrective Action Plan.

DBHDS has relied upon the adequacy of the CSB's corrective action plan and has considered this a crucial part of the risk assessment process. Written formal communication of this procedure indicating the acceptance or any required adjustment to the plan will be added to current procedures to ensure that the federal requirement of management decision is met.

Implementation of the response to this finding will be completed by June 30, 2016. The responsible parties ensuring that the implementation of this response are completed are Ken Gunn DBHDS Director, Office of Budget Operations and Financial Reporting and Randy Sherrod – DBHDS Director of Internal Audit.

Management Comment –Comply with the Code of Virginia Economic Interest Requirements:

The purpose of this memo is to provide the Department of Behavioral Health and Developmental Services (DBHDS) response to the management comment titled – Comply with the Code of Virginia Economic Interest Requirements. The Department concurs with the audit comment. DBHDS Office of Procurement and Administrative Services (OAS) tracks employee compliance of the Statement of Economic Interests reporting requirement using the Secretary of the Commonwealth's electronic system. Reminder emails are sent in advance of the reporting deadline to employees as needed. DHBDS, however, will increase the frequency used to monitor the online system. Further, DBHDS will increase the number of reminder emails sent through the Secretary of the Commonwealth's system to employees. Finally internal emails will be sent to stress the importance of the filing.

DBHDS will develop a tool to track and record employee attendance of the biennial Conflict of Interest training. Records will be maintained for five years. DBHDS was operating under the posted guidance from DHRM whereas this training was required of employees once.

Implementation of the response to this finding will be completed by June 30, 2016. The responsible party for ensuring implementation is the Director of Procurement and Administrative Services.

cc: Kathy Drumwright, DBHDS Interim Chief Deputy Commissioner
Connie Cochran, DBHDS Assistant Commissioner for Developmetal Services
Don Darr, DBHDS Assistant Commissioner for Finance, Administration and Technology
Daniel Herr, DBHDS Assistant Commissioner for Behavioral Health

Michael Schaefer, DBHDS Assistant Commissioner for Forensic Services
Tim Bass, DBHDS Chief Information Officer
Suzanne Battaglia, DBHDS Acting Chief Information Security Officer
Joe Cronin, DBHDS Director of Architectural and Engineering
Chris Foca, DBHDS Director of Procurement and Administrative Services
Ken Gunn, DBHDS Director of Budget and Financial Reporting
Stacy Pendleton, DBHDS Assistant Human Resources Director
Phil Peter, DBHDS Director of Fiscal Services & Grants Management
Randy Sherrod, DBHDS Internal Audit Director

COMMONWEALTH of VIRGINIA

Marissa J. Levine, MD, MPH, FAAFP
State Health Commissioner

Department of Health
P O BOX 2448
RICHMOND, VA 23218

TTY 7-1-1 OR
1-800-828-1120

January 7, 2016

Martha S. Mavredes, CPA
Auditor of Public Accounts
P.O. Box 1295
Richmond, VA 23218

Dear Ms. Mavredes:

We have reviewed your report on our audit for the year ended June 30, 2015. We concur with the findings, and a copy of our corrective action plan has been provided under a separate cover memo.

Regarding APA's Risk Alert to Upgrade or Decommission End-of-Life Server Operating Systems, the Virginia Department of Health began the Windows 2003 upgrade project on April 16, 2014. At that time, over 150 servers were running Windows 2003. Our goal was to not only to upgrade the servers to Windows 2012, but also consolidate, virtualize, or relocate servers whenever possible to the Chesterfield Enterprise Services Center. The assigned project manager was responsible for managing the coordination of server upgrades with the VDH Offices and Health Districts, implementing and submitting work requests to VITA/NG for the upgrades, and ensuring that all work was done on schedule and on budget. We are on track to complete this project in the next 30 days, with only 2 Windows 2003 servers remaining at this time.

We appreciate your team's efforts and constructive feedback. Please contact Alvie Edwards, Internal Audit Director, if you have any questions regarding our corrective action plan.

Sincerely,

Marissa J. Levine, MD, MPH, FAAFP
State Health Commissioner

VDH VIRGINIA DEPARTMENT OF HEALTH
Protecting You and Your Environment
www.vdh.virginia.gov

COMMONWEALTH of VIRGINIA

Department of Medical Assistance Services

CYNTHIA B. JONES
DIRECTOR

SUITE 1300
600 EAST BROAD STREET
RICHMOND, VA 23219
804/786-7933
800/343-0634 (TDD)
www.dmas.virginia.gov

January 5, 2016

Ms. Martha S. Mavredes
The Auditor of Public Accounts
P. O. Box 1295
Richmond, Virginia 23218

Dear Ms. Mavredes:

We have reviewed your draft audit report findings for the Department of Medical Assistance Services (DMAS) to be included in the report for the Audit of the Agencies of the Secretary of Health and Human Resources for the Fiscal Year Ending June 30, 2015. We concur with the audit findings assigned to DMAS. Attached please find the Department's Corrective Action Plan for the DMAS FY 2015 audit findings.

We appreciate the collaborative effort and the constructive feedback from your audit team during this year's audit. If you have any questions, please do not hesitate to contact our Director of Internal Audit, Paul Kirtz.

Sincerely,

Cynthia B. Jones

Department of Medical Assistance Services
APA Audit of the DMAS for the Fiscal Year Ending June 30, 2015
Corrective Action Plan
January 5, 2015

Create Formal Documentation that Facilitates Controlling Privileges in the Medicaid Management Information System – Repeat (issued as MP #5)

Condition

DMAS does not maintain detailed and accurate documentation of each employee's privileges in the Medicaid Management Information System (MMIS). Additionally, DMAS has not developed a conflict matrix, documenting the combinations of privileges that create internal control weaknesses.

Recommendation

DMAS should continue working towards properly documenting and evaluating MMIS Access by:

- Documenting privileges and conflicts in MMIS and providing a listing of users and these privileges to system owners and managers.
- Developing an automated process to more efficiently document MMIS privileges and provide a listing of users and these privileges to system owners and managers.
- Requiring systems owners to provide supervisors and the Information Security Officer documentation that facilitates them in evaluating current access and future requests.
- Requiring systems owners to train supervisors on the different privileges they are allowed to request.

Corrective Action Plan:

The DMAS Office of Compliance and Security (OCS) plans the following steps to address the APA recommendations:

1. The MOU between DMAS and DSS was modified in April 2015 to require DSS to complete an annual review of all DSS MMIS users. OCS created a listing of DSS users with the associated privileges and has been working with DSS since October 2015 for the access review and expects to complete the review by February 2016.
2. OCS has produced reports from MMIS that list all other systems users (except DSS users) with the associated privileges. OCS will stagger distribution of the reports to the division managers/supervisors to review and confirm user assignment, beginning in January 2016. OCS will advise the supervisors and managers how to assign and approve privileges for their staff in MMIS. Division managers/supervisors will either respond with modifications to OCS to make changes or will respond that employee access is appropriate. (Estimated Completion Date: May 31, 2016)

Department of Medical Assistance Services
APA Audit of the DMAS for the Fiscal Year Ending June 30, 2015
Corrective Action Plan
January 5, 2015

3. After the reviews are completed by May 31, 2016, OCS will provide formal training to DMAS directors, managers, and supervisors to ensure an agency-wide understanding of MMIS user privileges assigned by the supervisors and managers. (Estimated Completion Date: September 30, 2016)

In the long term, DMAS plans to purchase a COTS product to more efficiently document MMIS privileges and automate the distribution of listings of users and associated privileges to system owners and managers; however, the purchase has been delayed due to the ongoing work toward developing the Medicaid Enterprise System (MES) RFP (MMIS replacement). In order to integrate a COTS product into the future MES environment, a COTS purchase may not occur until the end of 2017.

Responsible Persons:

- Mukundan Srinivasan, DMAS Chief Information Officer, Information Management Division;
- Theresa Fleming, DMAS Information Security Officer, Office of Compliance and Security

Estimated Implementation Date: September 30, 2016

Develop Oracle Conflict Matrix – Repeat (issued as MP #2)

Condition

DMAS has recently documented conflicting modules or responsibilities within Oracle; however, DMAS has not yet used the conflict matrix to evaluate segregation of duties controls.

Recommendation

DMAS should continue to incorporate the conflict documentation into its access evaluations in a way that will allow managers to adequately evaluate the reasonableness of each employee's access to ensure proper segregation of duties surrounding fiscal transactions. After management completes their implementation of their new control, we will review their operating effectiveness in future audits.

Corrective Action Plan:

The DMAS Fiscal and Purchases Division (Fiscal) will incorporate the conflict matrix documentation into the following processes:

1. Approving requests for an employee to have Oracle Financials System access.

2. Performing access evaluations in the annual Oracle Financials security access reviews.

Department of Medical Assistance Services
APA Audit of the DMAS for the Fiscal Year Ending June 30, 2015
Corrective Action Plan
January 5, 2015

Fiscal initially used the conflict matrix on October 23, 2015 when adding a new employee on the Oracle Financials System and will continue to use it when adding the new system users.

Responsible Persons:

- Karen Stephenson, DMAS Fiscal and Purchases Division, Controller;
- Jonathan Dodd, DMAS Fiscal and Purchases Division, Fiscal Systems Administrator

Estimated Implementation Date: The corrective action plan (CAP) was partially completed beginning on October 23, 2015, when initially used for employee requests for Oracle Financials System Access. Full implementation is expected on June 30, 2016, the date for annual Oracle Financials security access reviews.

Limit Access to 1099 Adjustment and Reporting System (issued as MP #1)

Condition

DMAS Commonwealth Accounting and Reporting System (CARS) Security Officer did not remove access to the 1099 Adjustment and Reporting Systems (ARS), a subsystem of CARS, for individuals which no longer needed access. Seven of thirteen employees we tested retained 1099 Inquiry Function Access when it was no longer needed to perform their job responsibilities.

Recommendation

The CARS Security Officer should confer with Accounts to gain a better understanding of the ARS access information available to DMAS and use this understanding to perform comprehensive reviews of access in order to ensure that employees do not have unnecessary access to ARS.

Corrective Action Plan:

Corrective Action is complete. Seven of the thirteen employees referenced in the finding had their ARS Access removed on August 22, 2015.

On October 23, 2015, the CARS Security Officer conferred with a Department of Accounts General Accounting representative and obtained a detailed report of ARS access and used it when performing a comprehensive review for the CARS Security Certification. Utilizing the detailed report from DOA will continue with every review of CARS Access Security.

Controls Implemented

The Fiscal Policy & Procedure Manual has been updated to include specifics for granting CARS Security access and for the semiannual review process relating to ARS access and obtaining detailed data.

Department of Medical Assistance Services
APA Audit of the DMAS for the Fiscal Year Ending June 30, 2015
Corrective Action Plan
January 5, 2015

Responsible Persons:

- Karen Stephenson, DMAS Fiscal and Purchases Division, Controller;
- Jonathan Dodd, DMAS Fiscal and Purchases Division, Fiscal Systems Administrator

Implementation Date: October 23, 2015

Correct Operating Environment and Security Issues Identified by their Security Compliance Audit – Repeat (issued as MP #6)

Condition

The DMAS Internal Audit Division's review, dated January 31, 2014, found 15 exceptions in which the agency did not comply with the VITA Information Security Standard (SEC 501-7.1) and Health Insurance Portability and Accountability Act (HIPAA) Security Rule. According to management's updated correction plan, dated September 14, 2015, the following four exceptions remain, which they expect to address by the dates listed:

- Risk Assessment Procedures – March 31, 2016
- Logical Access Controls - December 31, 2016
- Training Materials - January 31, 2016
- Policies and Procedures Reviews - December 31, 2016

Recommendation

We recommend that DMAS continue to follow its updated corrective action plans for the identified weaknesses, which includes developing or acquiring the necessary resources to ensure that appropriate controls are applied over its sensitive information systems and data. In addition, as DMAS addresses these weaknesses, the agency should consider the most current security standard, SEC 501-09.

Corrective Action Plan:

Of the original 15 audit findings, 11 CAPs were previously completed. CAPs for the four remaining findings from the DMAS Internal Audit Security Compliance Audit have been revised to include recent status with completion milestones.

Risk Assessment Procedures

In 2014, DMAS hired a third party contract vendor, Assura, Inc., to conduct a full risk assessment and a business impact analysis using the most current Commonwealth Security Policy. Assura is on target to complete this project by the end of March 2016. After the completion of the risk

Department of Medical Assistance Services
APA Audit of the DMAS for the Fiscal Year Ending June 30, 2015
Corrective Action Plan
January 5, 2015

assessment, DMAS will develop a process to address the risks identified in the assessment. (Estimated completion Date: March 31, 2016)

Logical Access Controls

OCS has taken steps to strengthen controls for granting access to DMAS applications. The ISO trained a back-up ISO to help process access request forms. OCS will not grant access to systems without a signed access agreement.

When an employee is terminated, the supervisor must complete an Exit Clearance Form with a checklist that includes obtaining an approval sign-off from OCS to remove user access. When OCS receives the Exit Clearance Form, they notify VITA to suspend the network account. OCS is responsible for suspending the MMIS account. When HR sends emails about staff changes, OCS performs a cross-check to see if it has received and processed the Exit Clearance Form.

Once OCS completes MMIS user access reviews, OCS will produce reports that list all other systems users (excluding MMIS users) with the associated privileges. OCS will stagger distribution of the reports to the application system's owner to review and confirm user assignment, beginning in June 2016. The application system's owner will either respond with modifications to OCS to make changes or will respond that employee access is appropriate. (Estimated Completion Date: December 31, 2016)

In the long term, DMAS plans to purchase a COTS product to more efficiently document privileges internal applications and automate the distribution of listings of users and associated privileges to system owners and managers; however, the purchase has been delayed due to the ongoing work toward developing the Medicaid Enterprise System RFP (MMIS replacement). In order to integrate a COTS product into the evolving DMAS environment, a COTS purchase may not occur until the end of 2017.

Training Materials

OCS is scheduled to complete the update to the training materials on the Managed Online Awareness Training (MOAT) by January 31, 2015. The updates will address the concepts of separation of duties and intellectual property rights. (Estimated Completion Date: January 31, 2016)

Policy and Procedures Review

Part of the work that Assura, Inc. is completing will include a gap analysis on DMAS's policy and procedures and the requirements of the Commonwealth Security Standards (SEC 501-08 and SEC 501-09). The work is on target to be completed by March 31, 2016. OCS will use this analysis to update the security policy and procedures to ensure they are in compliance with the Commonwealth Security Standards. (Estimated Completion Date: December 31, 2016)

Department of Medical Assistance Services
APA Audit of the DMAS for the Fiscal Year Ending June 30, 2015
Corrective Action Plan
January 5, 2015

Responsible Persons:

- Mukundan Srinivasan, DMAS Chief Information Officer, Information Management Division;
- Theresa Fleming, DMAS Information Security Officer, Office of Compliance and Security
-

Estimated Implementation Date: December 31, 2016

Document *my*VRS Navigator Reconciliations (issued as MP #4)

Condition

DMAS' Human Resources Division is not adequately documenting reconciliations between its internal human resources records and the Virginia Retirement System (VRS) *my*VRS Navigator system, which contains essential retirement data for state employees. Additionally, management has not created policies or procedures detailing who needs to complete which steps to ensure reconciliations, changes, and adjustments for *my*VRS Navigator are performed accurately.

Recommendation

DMAS' Human Resources Division should develop *my*VRS Navigator policies and procedures to ensure compliance with *my*VRS Navigator requirements. Additionally, the Human Resources Division should ensure its internal human resources data and *my*VRS Navigator properly reconcile and retain sufficient documentation to demonstrate the identification and correction of reconciling discrepancies.

Corrective Action Plan:

DMAS' Human Resources Division has begun development of internal policies and procedures to ensure compliance with *my*VRS Navigator requirements. A step-by-step manual will be available for cross-training and to ensure the process is well-documented. Additionally, the Human Resources Division will ensure its internal human resources data and *my*VRS Navigator properly reconciles. Because of past issues with the *my*VRS Navigator and PMIS interface, whenever issues arise, the Operations Manager immediately addresses each with VRS. DMAS will develop a form to be completed for the reconciliation process to provide sufficient documentation of the reconciliation. That documentation will be retained in confidential files in the Operations Unit and will demonstrate the identification and correction of reconciliation discrepancies.

Responsible Persons:

- Kathleen B. Guinan, DMAS Human Resources Division Director;
- Patricia B. Pride, DMAS Human Resources Division, Benefits & Operations Manager

Estimated Implementation Date: April 1, 2016

Department of Medical Assistance Services
APA Audit of the DMAS for the Fiscal Year Ending June 30, 2015
Corrective Action Plan
January 5, 2015

Improve Access Management for the eVA System (issued as MP #3)

Condition

DMAS is not ensuring that employees have proper access within the eVA procurement system. DMAS did not formally designate its eVA Security Officers nor did it perform 75% of the required quarterly access reviews during fiscal year 2015. In addition, 2 out of 13 employees retained roles that were inappropriate for their job responsibilities.

Recommendation

DMAS should identify its Security Officers through appropriate designation forms and perform the required quarterly access reviews. Security Officers and all other employees should only have access levels appropriate for them to perform their assigned job duties. To achieve this, DMAS should allocate appropriate resources and consult with the Department of General Services to gain an understanding of eVA security standards and procedures, critical eVA controls, and employee access levels.

Corrective Action Plan:

The OCS Information Security Manager (ISO) is coordinating the identification of DMAS eVA security officers through appropriate eVA Designation forms. DMAS developed the following steps:

1. The DMAS ISO met with the two divisions that access the eVA System, Budget and Fiscal. Each identified primary and secondary leads within their Divisions. We also discussed the purchase level of authority for the Budget and Fiscal leads. The ISO also identified two backup security officers for OCS. (Completed December 17, 2015)

2. The ISO consulted with the Department of General Services to gain an understanding of eVA security standards and procedures, critical eVA controls, and employee access levels. Based on DGS' instructions the ISO is preparing the eVA Designation forms. She will then obtain appropriate signatures/approvals and file those with DGS for review. (Estimated Completion Date: January 31, 2016)

3. Obtain documentation of DGS approval of the eVA Designation forms. (Estimated Completion Date: February 29, 2016)

4. The ISO will develop an internal checklist for use when performing eVA Quarterly Access Reviews and train the Backup ISOs to conduct the review process. (Estimated Completion Date: January 31, 2016)

5. The ISO will perform and document the Quarterly Access Reviews beginning with the Quarter ending December 31, 2015. (Estimated Completion Date: January 31, 2016)

Department of Medical Assistance Services
APA Audit of the DMAS for the Fiscal Year Ending June 30, 2015
Corrective Action Plan
January 5, 2015

Responsible Persons:

- Karen Stephenson, DMAS Fiscal and Purchases Division, Controller;
- Theresa Fleming, DMAS Information Security Officer, Office of Compliance and Security

Estimated Implementation Date: February 29, 2016

COMMONWEALTH of VIRGINIA

DEPARTMENT OF SOCIAL SERVICES

Office of the Commissioner

Margaret Ross Schultze
COMMISSIONER

January 7, 2016

Ms. Martha Mavredes
Auditor of Public Accounts
101 North 14th Street
Richmond, VA 23219

Dear Ms. Mavredes:

Attached please find the Virginia Department of Social Services Response and Plan of Correction to the 2015 review of the Department by the Auditor of Public Accounts.

We concur with the audit findings and look forward to working with you on implementation of this plan.

Should you require additional information, please do not hesitate to contact Jack B. Frazier, Deputy Commissioner, Operations, by e-mail at jack.b.frazier@dss.virginia.gov or at (804) 726-7384.

Sincerely,

Margaret Ross Schultze

801 East Main Street • Richmond, VA 23219-2901
www.dss.virginia.gov • 804-726-7011 • TTY Dial 711

AGENCY OFFICIALS

As of June 30, 2015

Department of Medical Assistance Services
Cynthia B. Jones – Director

Department of Social Services
Margaret R. Schultze – Commissioner

Department of Behavioral Health and Developmental Services
Debra Ferguson, Ph.D. – Commissioner

Department of Health
Marissa Levine, M.D., MPH – Commissioner