



DEPARTMENTS FOR AGING
AND REHABILITATIVE SERVICES
AND THE BLIND AND VISION IMPAIRED

DISABILITY INSURANCE/ SOCIAL SECURITY INCOME
AGING CLUSTER
VOCATIONAL REHABILITATION
FEDERAL PROGRAMS

REPORT ON AUDIT
FOR THE YEAR ENDED
JUNE 30, 2016

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



AUDIT SUMMARY

Our audit of the Disability Insurance/Social Security Income, Aging Cluster, and the Vocational Rehabilitation federal programs, administered by the Department for Aging and Rehabilitative Services and the Department for the Blind and Vision Impaired for the fiscal year ended June 30, 2016, found:

- proper recording and reporting of all transactions, in all material respects, in the Commonwealth Accounting and Reporting System, Cardinal, and the Financial Reporting Transaction Entry Application;
- two matters involving internal control and its operations necessary to bring to management's attention; and
- two instances of noncompliance with applicable laws and regulations or other matters that are required to be reported.

The Aging Cluster consists of the following programs: Title III Part B Grants for Supportive Services and Senior Centers, Title III Part C Nutrition Services, and Nutrition Services Incentive Program.

–TABLE OF CONTENTS–

	<u>Pages</u>
AUDIT SUMMARY	
AUDIT FINDINGS AND RECOMMENDATIONS	1-3
INDEPENDENT AUDITOR’S REPORT	4-6
AGENCY RESPONSE	7
AGENCY OFFICIALS	8

AUDIT FINDINGS AND RECOMMENDATIONS

Continue to Improve IT Governance

Type of Finding: Internal Control and Compliance

The Department for Aging and Rehabilitative Services (Aging and Rehabilitative Services) is making progress to improve its information technology (IT) governance structure since the 2014 audit; however, various weaknesses continue to exist. The process is taking several years because the resources required to align its security policies and controls with the Commonwealth's Information Security Standard, SEC 501-09 (Security Standard) are extensive, resulting in Aging and Rehabilitative Services having to balance the use of its IT resources between policy development and execution and management of the IT security program. During the 2014 audit, we identified that Aging and Rehabilitative Services did not maintain appropriate oversight over its information security program, did not use some required controls to secure mission critical databases, and did not have an adequate risk management process. We identified and communicated these weaknesses to management during the 2014 audit 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. We did not perform detailed testwork on the identified issues in the current audit because Aging and Rehabilitative Services has not reached the corrective action due dates yet; however, we plan to review the status of each weakness during the next audit in Spring 2017.

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.

Aging and Rehabilitative Services should continue to dedicate the necessary resources to implement the controls discussed in the prior audit findings and continue to align Aging and Rehabilitative Service's operations with industry best practices and the Security Standard. The information security program control deficiencies that illustrate Aging and Rehabilitative Services' need to improve its IT governance are discussed below.

Continue to Improve Information Security Program

Aging and Rehabilitative Services is not maintaining sufficient oversight over the information security program to ensure it meets or exceeds the requirements of the Security Standard. Aging and Rehabilitative Services has made progress, but the IT Policy Manual is not complete, references an out-of-date Security Standard, and has no management approval.

The Security Standard requires the ISO to develop and manage an information security program that meets or exceeds the requirements of the Commonwealth's security policies and standards in a manner commensurate with risk.

Aging and Rehabilitative Services should evaluate its IT resource levels to ensure sufficient resources are available to implement and maintain an information security program. Aging and

Rehabilitative Services should also identify any additional training required to effectively and efficiently manage its information security program.

Improve Database Security

Aging and Rehabilitative Services does not use some required controls to protect a database that supports a critical system in the IT environment. The database contains sensitive information, such as personally identifiable information and operational data. We identified and communicated the weak controls to management during the 2014 audit 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 specific descriptions of security mechanisms.

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.

Aging and Rehabilitative Services should continue to dedicate the necessary resources to implement the controls discussed in the communication marked FOIAE and create a standard installation and configuration guide for its sensitive database that, at a minimum, meets the requirements in the Security Standard.

Improve Risk Management Process

Aging and Rehabilitative Services does not have a risk management process to support and protect its sensitive systems. Aging and Rehabilitative Services submitted a three-year risk assessment plan to the Virginia Information Technologies Agency (VITA). VITA approved the plan and Aging and Rehabilitative Services will execute the plan to bring its risk management process in compliance with the Security Standard. We identified and communicated the weak controls to management during the 2014 audit 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 specific descriptions of security mechanisms.

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

Aging and Rehabilitative Services should continue to work on the risk assessment plan for its sensitive systems and ensure their risk management process complies with the requirements in the Security Standard. Aging and Rehabilitative Services should evaluate whether the proper technical resources are in place to execute the risk management process.

Perform Annual Review of AWARE System Access

Type of Finding: Internal Control and Compliance

Aging and Rehabilitative Services' Information Security Team did not perform an annual review of access to the case management system, AWARE. The individual responsible for the review did not have adequate time to complete the review due to competing job responsibilities. Furthermore, a member of the Information Security Team made changes to their own AWARE access. Aging and Rehabilitative Services' AWARE security policy does not address whether members of the Information Security Team should make changes to their own accounts. Aging and Rehabilitative Services, Wilson Workforce and Rehabilitation Center, and the Department for the Blind and Vision Impaired use AWARE to document eligibility determinations, services planned for clients, and payment authorizations. In state fiscal year 2016, Aging and Rehabilitative Services' made over \$18 million in payments for services to individuals.

The Security Standard, Section AC-6 part 7, requires the performance of an annual review of access to validate that the need still exists and Section AC-5 requires separation of duties to prevent malevolent activity without collusion.

The Information Security Team should ensure that they review access annually to identify unnecessary access due to terminations or changes in job responsibilities. The Information Security Team should ensure that they have adequate staff to perform the annual review of the AWARE system. Furthermore, the Information Security Team should clarify the review policy to identify the specific time when the annual review should occur. The Information Security Team should ensure that all information system security policies address separation of duties. The lack of review and inadequate separation of duties puts the agency at risk for undetected and unauthorized use, which could result in an increase of fraud and abuse related to vocational rehabilitation eligibility determinations and payment authorizations.



Martha S. Mavredes, CPA
Auditor of Public Accounts

Commonwealth of Virginia

Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

January 20, 2017

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 **Disability Insurance/Social Security Income, Aging Cluster, and the Vocational Rehabilitation federal programs**, administered by the Department for Aging and Rehabilitative Services (Rehabilitative Services) and Department for the Blind and Vision Impaired (Blind and Vision Impaired), for the year ended June 30, 2016. We conducted this audit in accordance with auditing standards generally accepted in the United States of America and the standards applicable to financial audits contained in Government Auditing Standards, issued by the Comptroller General of the United States, in support of the Commonwealth's Single Audit. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions. 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 audit the Disability Insurance/Social Security Income, Aging Cluster, and the Vocational Rehabilitation federal programs in support of the Commonwealth's Single Audit. In support of this objective, we evaluated the accuracy of recorded financial transactions in the Commonwealth Accounting and Reporting System, Cardinal, and the Financial Reporting and Transaction Entry Application and in supplemental information submitted to the Department of Accounts. We reviewed the adequacy of the Rehabilitative Services and Blind and Vision Impaired's internal controls over the federal program and tested for compliance with applicable laws, regulations, contracts, and grant agreements. Rehabilitative Services transitioned to using Cardinal, the Commonwealth's new accounting and financial reporting system, on February 1, 2016.

Audit Scope and Methodology

Rehabilitative Services and Blind and Vision Impaired's 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 materiality and risk in determining the nature and extent of our audit procedures. Our review encompassed controls over the Disability Insurance/Social Security Income, Aging Cluster, and the Vocational Rehabilitation federal programs.

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

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

Conclusions

We found that Rehabilitative Services and Blind and Vision Impaired properly stated, in all material respects, the amounts recorded and reported in the Commonwealth Accounting and Reporting System, Cardinal, and the Financial Reporting and Transaction Entry Application and in supplemental information submitted to the Department of Accounts for the Disability Insurance/Social Security Income, Aging Cluster, and the Vocational Rehabilitation federal programs.

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 results for the Commonwealth's Single Audit for the year ended June 30, 2016, are contained in a separate report, which will be available on APA's website at www.apa.virginia.gov in February 2017.

Exit Conference and Report Distribution

We discussed this report with management on January 31, 2017. Management's response to the findings identified in our audit is included in the section titled "Agency Response." We did not audit management's response and, accordingly, we express no opinion on it.

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

DBC/alh



COMMONWEALTH OF VIRGINIA
DEPARTMENT FOR AGING AND REHABILITATIVE SERVICES

JAMES A. ROTHROCK
Commissioner

8004 Franklin Farms Drive
Henrico, VA 23229

Office (804) 662-7000
Toll free (800) 552-5019
TTY Toll free (800) 464-9950
Fax (804) 662-9532

January 23, 2017

Martha S. Mavredes, CPA
Auditor of Public Accounts
James Monroe Building
101 N. 14th Street
Richmond, Virginia 23219

Dear Ms. Mavredes:

We have reviewed your Single Statewide Audit Report for the Fiscal Year Ended June 30, 2016. We concur with the findings and are adopting strategies to improve the internal control environment of our agencies. Our responses are listed below.

Continue to Improve IT Governance

The agency concurs with this finding. We have completed all corrective action plans as of December 31, 2016, with the exception of the application risk assessments. We documented our risk assessment plan covering the period from July 1, 2016 to June 30, 2018 and submitted it to Commonwealth Security in June, 2016. The Plan was subsequently approved by Commonwealth Security and we are working to complete all risk assessments according to the plan.


Responsible Party: Mark McCreary, Information Security Officer
Estimated Completion Date: June 30, 2017

Perform Annual Review of AWARE System Access

The agency concurs with this finding and staff will no longer modify their own security, thereby ensuring proper controls over changes and separation of duties. Annual review of staff access will be performed in January of every year beginning in 2017 to validate the need still exists.

Responsible Party: Terry Johnson, IT Systems Analyst
Estimated Completion Date: March 31, 2017

Should you require more information, please do not hesitate to contact John Thaniel, Chief Financial Officer at john.thaniel@dars.virginia.gov or 804-662-7520.

Sincerely,

John W. Thaniel

dars@dars.virginia.gov · www.dars.virginia.gov

AGENCY OFFICIALS

As of June 30, 2016

James Rothrock, Commissioner
Department for Aging and Rehabilitative Services

Raymond Hopkins, Commissioner
Department for the Blind and Vision Impaired