VIRGINIA DEPARTMENT

OF

AGRICULTURE AND CONSUMER SERVICES

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

We have performed an audit of the following cycles at the Virginia Department of Agriculture and Consumer Services for the fiscal year ended June 30, 2016:

- payroll operations,
- information systems security, and
- procurement workflow controls.

Our audit found:

- proper recording and reporting of all transactions, in all material respects, in the Commonwealth's payroll system,

- matters involving internal control and its operation pertaining to information systems security necessary to bring to management's attention; and

- instances of noncompliance with applicable laws and regulations or other matters pertaining to information systems security that are required to be reported.

-TABLE OF CONTENTS-

AUDIT FINDINGS AND RECOMMENDATIONS

Continue to Improve IT Risk Management and Contingency Planning

The Virginia Department of Agriculture and Consumer Services (Department) is progressing; however, still does not have the necessary controls in their information technology (IT) risk management and contingency planning program to meet the requirements in the Commonwealth's Information Security Standard, SEC 501-09 (Security Standard). The Security Standard requires the Department to implement a complete and thorough risk management and contingency planning program to reduce risk, secure mission critical systems, and protect the confidentiality, integrity, and availability of sensitive data. Specifically, we found the following control deficiencies in the Department's IT risk management and contingency planning program.

Disaster Recovery Planning

The Department has a draft disaster recovery plan for IT systems; however, the plan is not final and does not have management's approval. In the event of a disaster, the Department will activate the draft plan; however, it does not meet the requirements in the Security Standard. The Department's draft Disaster Recovery Plan (DRP) does not identify recovery point objectives for the IT systems and does not include 11 systems that support a mission essential function as documented in the business impact analysis. Additionally, the Department has never conducted a full DRP test to confirm the plan's accuracy and effectiveness. They have also not stored a copy of the plan in a secure off-site location.

The Security Standard requires the development and testing of a disaster recovery plan that supports the restoration of business functions, including using data backups that are consistent with the defined recovery point objectives (*Security Standard: CP-1-COV-2 Contingency Planning Policies and Procedures, 3.2 Business Impact Analysis*).

Without a complete and approved disaster recovery plan that receives annual tests, the Department may not be able to restore mission essential business functions in a timely manner, which can lead to a disruption of services due mission critical and sensitive systems being unavailable.

The Department should finalize the disaster recovery plan and ensure it meets all requirements in the Security Standard and receive formal approval from management. Once the plan is complete and approved, the Department should conduct annual tests to confirm the effectiveness and validity of the plan to help ensure the availability of mission critical and sensitive systems in the event of a disaster.

Baseline Configuration Documentation

The Department does not have documented baseline configurations for their sensitive systems' hardware and software requirements. Baseline security configurations for application and database components are essential controls in IT environments to ensure that systems have appropriate configurations and serve as a basis for implementing or changing existing information systems. Without documented baseline configurations, the Department may not be able to restore mission critical systems to production status in a timely manner or confirm that systems are configured with the appropriate security controls.

The Security Standard requires baseline configurations, which include all the necessary information to restore these components back to production status in the event of a disaster. Some of the required information in a baseline configuration includes definition of required system components, required software packages, appropriate patch levels, security configurations, and required schema accounts (*Security Standard: CM-2 Baseline Configuration*).

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

IT Systems/Data Sensitivity Classifications

The Department does not consistently classify IT systems and data throughout the IT risk management documents and one system has the same individual designated in the role of Data Owner and System Administrator. Specifically, the Department classifies two systems as sensitive in the risk assessments, but does not classify the same systems as sensitive in the business impact analysis. Without consistent system and data sensitivity classifications the Department may not implement the proper controls to adequately protect sensitive systems.

The Security Standard requires the information in the business impact analysis to be used as the primary input for risk assessments, highlighting the importance of consistency between these artifacts. The Security Standard also requires separate individuals to have the roles of Data Owner and System Administrator to prevent a separation of duties issue (*Security Standard: 3.2 Business Impact Analysis, 2.4 Agency Head*).

The Department should ensure all sensitive systems and data are consistent throughout the IT risk management documents. The Department should also review the roles and responsibilities for each sensitive system to prevent any potential separation of duties issues. Having consistency throughout the IT risk management program will help to ensure the proper controls are in place to protect the agency's mission critical and sensitive data.

<u>Improve Database Security</u>

The Department does not secure the database supporting multiple mission critical and sensitive systems, including their primary financial management system, in accordance with agency policy, the Security Standard, and industry best practices. Sensitive systems, including the Department's financial system of record that interfaces financial information to the Commonwealth's accounting and financial reporting system, require strong security controls to protect the confidentiality, integrity, and availability of financial and sensitive data.

The Security Standard requires implementing specific controls to reduce unnecessary risk to data confidentiality, integrity, and availability. The Department upgraded the database to a newer version in the summer of 2016 and we noted nine areas related to the configuration of the database where the Department does not have sufficient controls, some of which are related to least functionality, account management, and system monitoring. We identified and communicated these specific control weaknesses 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.

By not meeting the minimum requirements in the Security Standard and aligning the database's settings and configurations with best practices, the Department cannot ensure data integrity within the database. Also, the Department may not identify malicious or fraudulent activity that is occurring within the database.

The Department should dedicate the necessary resources to configure appropriate security controls for the database in accordance with the Security Standard and industry best practices. Doing this will help maintain the confidentiality, availability, and integrity of the Department's sensitive and mission critical data.

Improve Oversight of Third-Party Service Providers

The Department does not maintain appropriate oversight for two independent third-party service providers that perform information security functions for a system that contains confidential personally identifiable information. As the System Owner, the Department is responsible to make sure the system meets or exceeds all security requirements defined in the Security Standard.

Specifically, the Department has not clearly defined the roles and responsibilities between the System Owner and the service providers. Also, the Department does not have any contractual language that requires the service providers to implement specific information security controls that meet or exceed the requirements defined in the Department's policies and the Security Standard. In addition, the Department does not have a sufficient process to gain assurance the information technology controls at the service providers are operating effectively.

The Security Standard requires the Department to ensure service providers comply with their security requirements and the requirements in the Security Standard. Additionally, the Security Standard requires the Department to define user roles and responsibilities with regard to external information system services and to employ appropriate processes to monitor security control compliance by the service providers on an on-going basis (*Security Standard: SA-9 External Information System Services*).

Due to a lack of oversight for the external service providers, three weaknesses were identified in the system that increase the risk to the confidentiality, integrity, and availability of sensitive data, which could lead to legal, financial, or reputational damages. We identified and communicated these specific control weaknesses 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 Department has a process that requires service providers to fill out a self-reported security checklist; however, this process does not meet the requirements in section SA-9 of the Security Standard. The Department does not have a sufficient process for maintaining oversight over service providers due to misunderstanding of Security Standard requirements.

The Department should dedicate the necessary resources to develop and implement a process to maintain appropriate oversight over external service providers. At a minimum, management should consider including the following elements in the process:

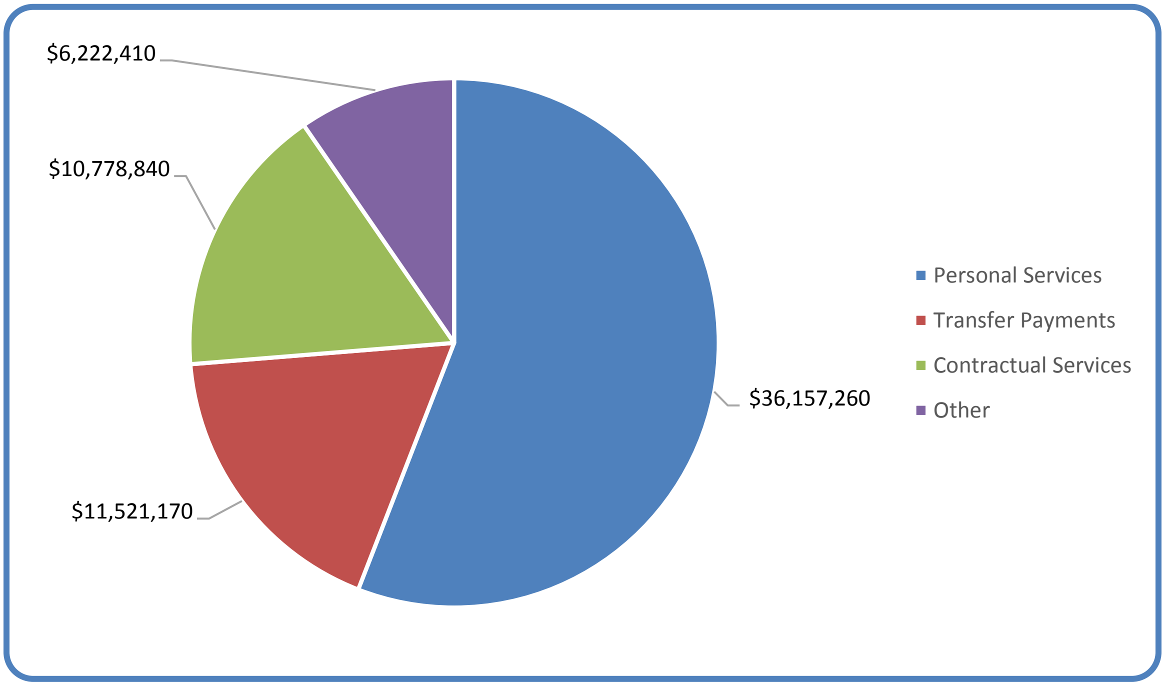
- Clear definition of roles and responsibilities for the Department and all service providers,
- Requirement for appropriate contractual language that requires service providers maintain controls that are compliant with organizational policies and the Security Standard, and
- Develop a process and define requirements for monitoring service providers for compliance with applicable organizational policies and the Security Standard.

The Department should also work with the appropriate service provider to implement mitigating controls until they remediate the risks identified in the FOIAE document. By implementing a sufficient process to gain assurance over their external service providers, the Department will help to ensure the confidentiality, integrity, and availability of sensitive data.

AUDIT SCOPE OVERVIEW

The Virginia Department of Agriculture and Consumer Services (Department) promotes the economic growth and development of Virginia agriculture, provides consumer protection, and encourages environmental stewardship. The Department employs approximately 500 salaried and 175 wage employees who work in various locations; personal services accounts for over half of the Department's expenses. Beginning January 1, 2015, the Department decided to begin processing all payroll internally. Prior to this date, the Department had outsourced its payroll processing operations to the Payroll Service Bureau, a service center at the Department of Accounts. As payroll is the Department's largest expense and the process is new to the Department since their prior audit, we included payroll operations as one of our objectives for this audit.

Expenses by Category for the year ended June 30, 2016



Source: The Commonwealth's accounting and financial reporting system

We also included Information Systems Security (ISS) as a primary objective during this audit. Our approach to identifying critical ISS work includes following up on prior year audit findings and reviewing all mission critical or sensitive systems for changes in their environments. We determined that recent upgrades of the database supporting multiple sensitive and mission critical applications, including the primary financial management system, were performed and; therefore, were reviewed during this audit. We also determined the system used by the Department to management its laboratory information contained sensitive information and had not been reviewed in recent audits. The Department relies on two third-party service providers to support and manage the system; therefore, they are required to maintain oversight for the security functions provided by these service providers. Further, as access control security provides the first line of defense for ISS, we tested access to multiple systems we deemed critical to other audit objectives. In combination, the follow-up on prior audit findings and the items mentioned above in the ISS scope provided reasonable assurance over key ISS security controls.

An additional objective included during this audit was procurement workflow controls. Contractual services, also a large expense category for the Department, are initially requested through the Commonwealth's procurement system. In testing procurement workflow controls, we ensured that controls over the procurement of these expenses were in place and functioning adequately.

Commonwealth of Virginia

Auditor of Public Accounts

Martha S. Mavredes, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

March 24, 2017

The Honorable Terence R. McAuliffe
Governor of Virginia

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

We have audited the payroll operations, information systems security, and procurement workflow controls of the **Virginia Department of Agriculture and Consumer Services** for the year ended June 30, 2016. 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 Scope and Objectives

Our audit's primary objectives were to audit the payroll operations, information systems security, and procurement workflow controls cycles. In support of these objectives, we evaluated the accuracy of recorded financial transactions in the Commonwealth's payroll system; reviewed the adequacy of the Department's internal controls over the specified cycles; and tested for compliance with applicable laws, regulations, and contracts agreements as they related to our objectives. We also reviewed corrective actions of audit findings from prior year reports.

Audit Methodology

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

We gained an understanding of the overall internal controls, both automated and manual, as they related to the audit objectives, sufficient to plan the audit. We considered significance and risk in determining the nature and extent of our audit procedures.

We performed audit tests to determine whether the Department's controls relating to our objectives were adequate, had been placed in operation, and were being followed. Our audit also included tests of compliance with provisions of applicable laws, regulations, and contracts as they related to our audit objectives. Our audit procedures included inquiries of appropriate personnel, inspection of documents, records, and contracts, and observation of the Department's operations. We performed analytical procedures and tested details of transactions to achieve our objectives.

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

Conclusions

We found that the Department properly stated, in all material respects, the amounts recorded and reported in the Commonwealth's payroll system relating to the audit objectives. The financial information presented in this report came directly from the Commonwealth's accounting and financial reporting system.

We noted certain matters involving internal control and its operation and compliance with applicable laws, regulations, and contracts pertaining to information systems security that require management's attention and corrective action. These matters are described in the section entitled "Audit Findings and Recommendations."

The Department has taken adequate corrective action with respect to the audit finding titled, "Improve Oracle Database Security" reported in the prior year. The Department's corrective action for "Perform Timely Updates to IT Risk Management and Contingency Plans" is on-going and is re-issued as a part of the current year finding, "Continue to Improve IT Risk Management and Contingency Planning".

Exit Conference and Report Distribution

We discussed this report with management on April 27, 2017. Management's response to the findings identified in our audit is included in the section titled "Department 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

AVC/clj

COMMONWEALTH of VIRGINIA

Sandra J. Adams
Commissioner

Department of Agriculture and Consumer Services
PO Box 1163, Richmond, Virginia 23218
Phone: 804/786-3501 • fax: 804/371-2945 • Hearing Impaired: 800/828-1120
www.vdacs.virginia.gov

May 3, 2017

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

Dear Ms. Mavredes:

We have reviewed the draft audit report covering the Virginia Department of Agriculture and Consumer Services ("the agency") and the Virginia Agricultural Council for the year ended June 30, 2016. In response to the findings, the agency is committed to maintaining secure data. The agency continues to dedicate both the available resources of its information systems staff and the internal auditor to assure overall compliance with statewide security standards. The agency maintains a strong risk assessment program and prioritizes each compliance requirement based on availability of resources.

Until recently, the agency has been unable to complete its disaster recovery plan due to VITA/NG's offerings being cost prohibitive for the actual services provided. Recently an option became available that will allow the agency to acquire services and comply with requirements. The agency anticipates finalizing the disaster recovery plan and testing it this calendar year. Work has already begun on resolving database security items and these are expected to be addressed and completed in the near future. The agency is in communication with VITA and other vendors to define roles and responsibilities related to third-party vendors. In addition, oversight processes will be developed to ensure compliance with the Security Standard. The agency anticipates a completion date prior to the next audit.

We appreciate the opportunity to respond regarding our efforts to continually improve the agency's security program.

Sincerely,

Sandra J. Adams
Commissioner

cc: The Honorable Basil I. Gooden, Secretary of Agriculture and Forestry

VIRGINIA DEPARTMENT OF AGRICULTURE AND CONSUMER SERVICES

(as of June 30, 2016)

BOARD MEMBERS

Steven W. Sturgis, President
Robert J. Mills, Jr., Vice-President
Kevin Schmidt, Secretary

O.Bryan Taliaferro, Jr.
Shelley S. Butler Barlow
Clifton A. Slade
Kevin J. Kordek
L. Wayne Kirby

John R. Marker
Kay Johnson Smith
Rosalea R. Potter
James S. Huffard, III
Richard S. Sellers

Neil Houff

EX-OFFICIO

Dr. Timothy D. Sands, President
Virginia Polytechnic Institute and State University

Dr. Makola M. Adbullah, President
Virginia State University

AGENCY OFFICIALS

Sandra J. Adams
Commissioner