MIKE HARMON
AUDITOR OF PUBLIC ACCOUNTS

February 7, 2019

William M. Landrum III, Secretary
Finance and Administration Cabinet
Room 383 Capitol Annex
Frankfort, KY 40601

Dear Secretary Landrum,

We have audited the Finance and Administration Cabinet (FAC) as an integral part of our audit of the Comprehensive Annual Financial Report (CAFR) for the year ended June 30, 2018. Our procedures included testing certain activities of FAC for compliance and internal control over financial reporting, and our findings and recommendations related to those procedures are reported as described below.

Internal Control

We considered FAC's internal control to determine the audit procedures that are appropriate in the circumstances for the purpose of expressing our opinion on the Commonwealth's financial statements, but not for the purpose of expressing an opinion on the effectiveness of internal control. Accordingly, we do not express an opinion on the effectiveness of the Commonwealth's or the FAC's internal control.

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct misstatements on a timely basis. A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance.

A material weakness is a deficiency, or combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected on a timely basis.

Our consideration of internal control was for the limited purpose described above and was not designed to identify all deficiencies in internal control that might be significant deficiencies or material weaknesses. All material weaknesses and significant deficiencies over financial reporting noted during our audit, including those related to the FAC, if any, are reported in the Statewide Single Audit of Kentucky (SSWAK) – Volume I. Control deficiencies identified in our audit for the FAC that were not classified as either significant deficiencies or material weaknesses are attached to this letter.

Compliance and Other Matters

As part of obtaining reasonable assurance about whether the Commonwealth’s financial statements are free of material misstatement, we performed tests of its compliance with certain laws, regulations, contracts and grant agreements, noncompliance with which could have a direct and material effect on the determination of financial statement amounts. However, providing an opinion on compliance with those provisions was not an objective of our audit, and accordingly, we do not express such an opinion. All material noncompliances, as well as material instances of fraud, abuse or other matters related to financial reporting noted during our audit, including those related to FAC, if any, are reported in the Statewide Single Audit of Kentucky (SSWAK) – Volume I.

Other noncompliances or other matters identified during our audit for FAC not classified as material are attached to this letter.

This communication is intended solely for the information and use of management, those charged with governance and others within the organization and is not intended to be and should not be used by anyone other than these specified parties.

Thanks and God Bless,

Mike Harmon
Auditor of Public Accounts

FINANCIAL STATEMENT FINDINGS

Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 18-COT-01: The Commonwealth Office Of Technology Did Not Ensure Policies And Procedures Were Updated Appropriately, Nor Developed A Privacy Policy Or Program

The Commonwealth Office of Technology (COT) has not reviewed or revised three Enterprise IT Policies and Standards (CIO-086, CIO-101, and CIO-102) in the past two years. COT has not developed an Enterprise Privacy Policy or Privacy Program. Two positions have been created and filled to help create a policy and program and a policy is already under development. However, the policy and program had not been developed or implemented prior to the end of fieldwork.

COT did not consistently review certain Enterprise IT Policies and associated procedures for accuracy to ensure current and relevant information is detailed for enterprise agencies. Furthermore, COT has not developed a privacy policy or program to guide agencies in protecting sensitive data.

Without clear, current, and accurate Enterprise Policies, agencies attempting to follow these procedures may become confused about their responsibilities or inappropriately develop procedures to adhere to outdated or incorrect policies. Furthermore, without a clear, current, and accurate privacy policy and program in place, agencies may not be able to sufficiently or effectively safeguard the collection, access, use, dissemination, and storage of personal or sensitive data and it is more likely breaches may occur that lead to the theft of personal or sensitive data.

Within each CIO Enterprise Policy:
Review Cycle: This policy will be reviewed at least every two years.
According to KRS 42.726:

> (1) The roles and duties of the Commonwealth Office Technology shall include but not be limited to:
> …
> (c) Developing strategies and policies to support and promote the effective application of information technology within state government as a means of saving money, increasing employee productivity, and improving state services to the public, including electronic public access to information of the Commonwealth;
> (d) Developing, implementing, and managing strategic information technology directions, standards, and enterprise architecture, including implementing necessary management processes to assure full compliance with those directions, standards, and architecture. This specifically includes but is not limited to directions, standards, and architecture related to the privacy and confidentiality of data collected and stored by state agencies;
> …
> (p) Preparing proposed legislation and funding proposals for the General Assembly that will further solidify coordination and expedite implementation of information technology systems

FINDING 18-COT-01: The Commonwealth Office Of Technology Did Not Ensure Policies And Procedures Were Updated Appropriately, Nor Developed A Privacy Policy Or Program (Continued)

Recommendation

We recommend COT review all Enterprise policies currently in effect to ensure they reflect management decisions, current operational structure, and required procedures. Going forward, these documents should be reviewed at least every two years, as designated in each policy, for accuracy of content and references to other documents, statutes, and regulations.

Additionally, we recommend COT continue to work with the Finance and Administration Cabinet, the Chief Data Officer, and the Chief Compliance Officer to ensure the completion of an Enterprise Privacy Policy and Privacy Program. COT should establish and implement a mechanism for monitoring the effectiveness and practice of the policy and program.

Management's Response and Planned Corrective Action:

The three referenced policies were identified and reviewed by the appropriate COT employees before the revision date. Two of the policies were identified as needing to be deleted, the third was identified for revision.

COT reviewed the policy adoption and review process and identified gaps that contribute to policy recommendations not being properly processed and policy recommendations not being addressed in a timely manner. COT has drafted a policy adoption and revision procedure and has placed the procedure in operation. Using this new business process all policies that have not been timely reviewed or that due review will be addressed by 12/31/2018.

On April 2, 2018, COT hired a Chief Compliance Officer. This individual is responsible for the functions described in NIST 800-53 rev4 Appendix J, AR-1. Effective 8/17/2018 COT adopted and published CIO-106 Enterprise Privacy Policy that is the foundation of the COT Privacy program. The following is a listing of the in-progress actions by COT to implement and support this privacy program:

Start of comprehensive review of all COT policies, including policies recommended for deletion. This process will be completed for all policies beyond the two-year review period by end of December, 2018

Develop a Privacy Impact Assessment and Business Impact Assessment. These documents are completed and a proof of concept is in process to test the effectiveness of the documents. The POC will end December 15, 2018. The revised documents will become part of the COT Privacy Program.

Management's Response and Planned Corrective Action (Continued):

To support a privacy program, the following needed documentation has been identified. All listed documentation is in draft format. The listed documents are scheduled to be finalized by June 30. 2019

Dashboard for tracking policy adoption process comments from stakeholders
Procedure: Privacy Documentation Procedures
Procedure: Individual Choice/Consent, Access, Correction and complaints
Procedure: Privacy Training and Awareness Plan
Procedure: Privacy Incident Response Plan
Procedure: COT policy adoption

The Chief Compliance Officer is sponsoring and providing support to all Executive Cabinets to adopt a Master Data Sharing Agreement. This documentation will provide the data privacy and security standards for Commonwealth data and will identify a Cabinet level employee as the point of contact for the Cabinet's data. The first signatories to the Master Data Sharing Agreement are expected by 12/31/2018.

Finally, besides the Chief Compliance Officer COT is developing the structure needed to support a Privacy and Audit Office. The Office is scheduled to be created by end of calendar year 2018. Personnel to assume privacy program functions will be transferred to these function by 9/15/18.

Auditor's Reply:

At the time fieldwork was completed, CIO-086 had a revision date of March 9, 2016 and CIO-101 and CIO-102 did not have a review or revision date recorded.

FINANCIAL STATEMENT FINDINGS

Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 18-DOR-01: The Department Of Revenue Did Not Completely Comply With Enterprise Policies And Standards To Protect Confidential And Sensitive Information

The Department of Revenue (DOR) has weak procedures over the security of confidential and sensitive data. DOR is required to follow Commonwealth Office of Technology (COT) enterprise policies and standards, and there are several policies and procedures that address data protection. DOR did not consistently follow these policies to ensure all data was fully protected. This security concern was originally identified and communicated to the agency during our FY 2013 audit.

Detailed information that could potentially increase the risk of agency security being compromised was intentionally omitted from this comment. However, auditors thoroughly discussed this issue with DOR.

DOR does not fully comply with CIO-092 Media Protection Policy. They have identified and classified their data, and adequately protected data in transit. However, to fully comply, data at rest must be properly protected. To do this, DOR must identify and purchase a tool or method for COT to implement and manage on their behalf. This has not been completed to date.

Also, since CIO-092 is an enterprise policy, COT has not enforced compliance with their own policy.

Failure to adequately protect data increases the risk that Personally Identifiable Information (PII) or other sensitive or confidential data could be accessed or made available to the general public, which could compromise information related to claimants, employees, or vendors and open the agency to potential lawsuits. Also, this could negatively impact the financial statements if confidential data is stolen, which could result in substantial mitigation and legal fees for the agency and/or taxpayer as well as loss of taxpayer trust and damage to the agency's reputation.

The COT Enterprise Policy, CIO-092 Media Protection Policy, states that information stored on digital media must comply with regulatory requirements listed in the 5100 Encryption Standard. The standard states that once data has been classified, the agency must determine the proper encryption implementations to achieve the desired level of protection for all data.

Recommendation

We recommend data classified as confidential or sensitive should be sufficiently protected in compliance with COT enterprise policies and standards. Management should ensure sufficient resources are dedicated to address this weakness in a timely manner and ensure the security of confidential and sensitive data remains a top priority. Further, management should provide training to staff, as needed, to ensure policies are consistently applied.

FINANCIAL STATEMENT FINDINGS

Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 18-DOR-01: The Department Of Revenue Did Not Completely Comply With Enterprise Policies And Standards To Protect Confidential And Sensitive Information (Continued)

Management's Response and Planned Corrective Action

There are compensating controls surrounding the servers that house DOR data to keep it secure while the agency researches the best way to protect the data. These controls include firewalls, restricted access rights which are required to access systems within security boundaries, user ID and password specifications, and a documented process for requesting access to systems.

DOR is continuing to work on testing systems to protect data at rest to meet the requirements.

FINANCIAL STATEMENT FINDINGS

Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 18-FAC-01: The Division Of Engineering And Contract Administration Did Not Comply With KRS 45A.095 When Processing Emergency Procurements

As part of the audit of the Commonwealth's comprehensive annual financial report, emergency procurements were reviewed. The Division of Engineering and Contract Administration (DECA) processes emergency procurements for Commonwealth construction projects. The following exceptions were identified during testing:

- One emergency procurement for $198,800 did not have documentation of approval by the Finance and Administration Cabinet (FAC) Secretary.
- One emergency procurement with an estimated cost of $300,000 for electrical work at the Commonwealth Office of Technology did not have documentation that met the definition of an emergency condition as defined in KRS 45A.095.

FAC approval and authorization was not obtained for the $198,000 project. For the $300,000 project, approval was requested and obtained. However, the review process did not ensure the situation met the definition of an emergency condition in KRS 45A.095.

Failing to seek approval or adequately document approval of emergency procurements creates a noncompliance with policies, procedures, and statutes governing procurement, and circumvents internal controls put into place by FAC to ensure state procurements follow the model procurement code.

FAP 220-11-00 states the following:

> (1) The Department for Facilities and Support Services shall assist the secretary of the Finance and Administration Cabinet in regard to emergencies, as defined in 45A.095(4) relating to construction.
> (4) The head of the agency shall provide documentation to the secretary of the Finance and Administration Cabinet that explains the emergency purchase and is approved or signed by the secretary of the cabinet involved or his designee…The secretary of the Finance and Administration Cabinet or his designee shall approve the purchase before payment authorization.

FINDING 18-FAC-01: **The Division Of Engineering And Contract Administration Did Not Comply With KRS 45A.095 When Processing Emergency Procurements (Continued)**

KRS 45A.095 states the following:

> (1) A contract may be made by noncompetitive negotiation only for sole source purchases, or when competition is not feasible, as determined by the purchasing officer in writing prior to award…or when emergency conditions exist.
> (3) "An emergency condition is a situation which creates a threat or impending threat to public health, welfare, or safety such as may arise be reason of fires, floods, tornadoes, other natural or man-caused disasters, epidemics, riots, enemy attack, sabotage, explosion, power failure, energy shortages, transportation emergencies, equipment failures, state or federal legislative mandates, or similar events. The existence of the emergency condition creates an immediate and serious need for services, construction, or items of tangible property that cannot be met through normal procurement methods and the lack of which would seriously threaten the functioning of government, the preservation or protection or property, or the health or safety of any person."
> (4)…The existence of the emergency shall be fully explained, in writing, by the head of the agency for which the purchase is to be made. The explanation shall be approved by the secretary of the Finance and Administration Cabinet, and shall be filed with the record of all such purchases and made available to the public.

Recommendation

We recommend DECA implement adequate internal controls to ensure emergency procurements are appropriately supported and approved in accordance with KRS 45A.095.

Management's Response and Planned Corrective Action

Management did not provide a response.

FINANCIAL STATEMENT FINDINGS

Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 18-FAC-02: The Finance And Administration Cabinet Did Not Inform eMARS Report Developers Of Unreliable Classes In eMARS Reporting And Did Not Update Statewide Reports To Exclude These Classes

Certain enhanced Management Administrative and Reporting System (eMARS) reports used by agencies for management and accounting purposes were unreliable. These reports are unreliable because two classes in the *FIN – General Accounting Universe* are unreliable and no longer necessary, but the Office of Statewide Accounting Services (SAS) in the Finance and Administration Cabinet (FAC) has not proactively worked to inform users and update reports.

Enterprise Business Intelligence (EBI) is a framework used by the Commonwealth to build and maintain reports. eMARS Reporting is a collection of report documents in EBI related to the eMARS financial system. FAC creates statewide reports and stores them in eMARS Reporting to be used by agencies as-is or as templates for customized reports. On May 21, 2018, FAC notified eMARS Report Developers that modified copies of the '2302 – Outstanding Encumbrance' statewide report were returning results that varied from the original report and that FAC had corrected this issue. The email distribution list used to notify the Report Developers was out of date and FAC asked recipients to forward the email as needed.

The '2302' report was written to pull amounts from the *Basic Accounting Ledger* class during the upgrade to eMARS 3.10, which was implemented on September 25, 2015. FAC no longer trains on the use of this class or the *Detailed Accounting Ledger* class as they can yield invalid results when searched for in conjunction with certain other fields. Instead, reports should be written to pull amounts from the *Accounting Journal* class, which does not encounter this issue.

In FY 2016, FAC provided documentation to support the testing conducted on the 152 statewide reports which were redeveloped for the eMARS 3.10 upgrade. The documentation was not complete and final due to the separation of the individual responsible for maintaining it, but FAC was not aware of any issues with the reports. As a result, a finding was issued recommending FAC maintain complete documentation going forward. The documentation from FY 2016 did not list the 2302 report, or 43 other reports, as having passed quality assurance (QA) testing. During the current engagement FAC staff reviewed these 43 reports and determined that three of these reports were also pulling from the *Basic Accounting Ledger* class and would be corrected. The reports were: '1540S – Allotment Summary', '3010A – Payroll Summary Charges by Department', and '3010B – Payroll Summary Charges by Cabinet and Department'.

FINANCIAL STATEMENT FINDINGS

Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 18-FAC-02: The Finance And Administration Cabinet Did Not Inform eMARS Report Developers Of Unreliable Classes In eMARS Reporting And Did Not Update Statewide Reports To Exclude These Classes (Continued)

The *Basic Accounting Ledger* and *Detailed Accounting Ledger* classes were introduced in 2006. The vendor for eMARS warned FAC these classes would produce inconsistent results if not used appropriately. Instead, the *Accounting Journal* class should be used to ensure there were no errors. At the time, there were severe performance issues with infoAdvantage, the predecessor to eMARS Reporting. Because reports using the *Basic and Detailed Accounting Ledger* classes ran much faster than those using the *Accounting Journal* class, which would often timeout, FAC determined the inconsistencies with these classes were an acceptable risk. The classes were introduced into the *FIN – General Accounting Universe* and eMARS Report Developers were trained on how to appropriately use them. Improved database indexing has eliminated the performance issues and there is no longer a need to use the *Basic and Detailed Accounting Ledger* classes.

Due to performance issues with the reporting solution in 2006, Finance accepted the risk associated with the use of the *Basic Accounting Ledger* and *Detailed Accounting Ledger* classes. Users were trained on how to properly use these classes to pull reports at that time. Significant turnover across state government has been occurring over the past few years. As such, this has resulted in the loss of this knowledge. Finance has not maintained an up to date list of properly trained eMARS Report Developers.

Depending on the use of the report, errors may occur in the financial statements or an agency may be out of compliance with statutes or regulations. For example, if an agency used an incorrect report to perform reconciliations, the agency may create an entry in eMARS to correct a discrepancy that does not actually exist. In addition, an agency could use an incorrect report for federal reimbursements.

Reports should be accurate for financial, compliance, and management purposes. According to COBIT 5 – Evaluate, Direct and Monitor – EDM01.02 Direct the governance system:

“4. Ensure that communication and reporting mechanisms provide those responsible for oversight and decision-making with appropriate information.”

According to ‘Appendix C – Accounting Journal vs. Summary Ledgers’ of the ‘eMARS Thick Client Reporting’ training provided to eMARS Reporting users in 2006:

> “Rule of thumb for deciding where to pull Dimension, Detail, or Measure Objects is as such:
>
> 1. If you need document level detail, always start with the Accounting Journal Class…
>
>   c. Do not pull Posting Amount from either Basic or Detailed Accounting Ledger, instead pull Pstng Amount from the Accounting Journal Class…
>
> 3. If you do not need document level detail or any of the Dimension, Detail or Measure Objects found in the Accounting Journal Class or Document Class, pull Posting Amount from one of the Accounting Ledger Classes; because, summary ledgers only contain rollup information…

FINDING 18-FAC-02: The Finance And Administration Cabinet Did Not Inform eMARS Report Developers Of Unreliable Classes In eMARS Reporting And Did Not Update Statewide Reports To Exclude These Classes (Continued)

> If you need a report that shows document level detail, you have to use either the Accounting Journal Class or the Document Class. However, if you do not need document level detail, you may use either the Basic or Detailed Accounting Ledger to pull Posting Amount.
>
> If you decide you do not need document level detail and use Posting Amount from either the Basic or Detailed Accounting Ledger Class, you need to make sure you only use Dimension Objects and their corresponding Detail Objects in your query that are listed in this document."

Recommendation

We recommend FAC compile a current listing of all eMARS Report Developers and update their distribution lists accordingly. FAC should notify these users that the *Basic Accounting Ledger* and *Detailed Accounting Ledger* classes are no longer reliable and to update their reports to use the *Accounting Journal* class as necessary. FAC should review the statewide reports, and any other reports they use, to ensure all reports have been updated to pull from the *Accounting Journal* class. Once the reports have been updated, FAC should remove the *Basic and Detailed Accounting Ledger* classes or hide them from users.

FAC should continue to develop and provide eMARS and eMARS Reporting training to users to mitigate risks associated with employee turnover. In addition, Finance should continue to document issues noted with reports and communicate these issues with eMARS Report Developers as appropriate. Changes to reports should be developed, tested, and implemented as necessary. All documentation should be complete and maintained for management and auditing purposes.

Management's Response and Planned Corrective Action

Quality Assurance efforts for past upgrades have been geared primarily toward ensuring that Statewide Reports produce results which are financially accurate and do not materially differ from those produced by the same reports in the prior upgrade. The Statewide Reports were tested according to this guiding principal for both the eMARS 3.10 upgrade (as documented in the 2016 information provided) and the eMARS 3.11.1 upgrade (as documented in 2018 information provided).

FINANCIAL STATEMENT FINDINGS

Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 18-FAC-02: The Finance And Administration Cabinet Did Not Inform eMARS Report Developers Of Unreliable Classes In eMARS Reporting And Did Not Update Statewide Reports To Exclude These Classes (Continued)

Management's Response and Planned Corrective Action (Continued)

More recently, in addition to maintaining the existing Statewide Reports, greater attention has been placed on agency reporting needs. A team which includes agency representatives has been organized to provide feedback on the reporting process which can be factored into prioritization of efforts in this area moving forward.

As such, below are target dates for the effort to address this finding:

Target Date	Implementation Step	Notes/Considerations
9/14/2018	Test ability to hide classes without "breaking" reports to prevent new reports being developed to use them	Pending universe name changes scheduled for completion by 8/31/2018
9/21/2018	Hide the Basic Accounting Ledger and Detail Accounting Ledger classes in the universes	Assuming this can be done without preventing existing reports from being refreshed or modified
9/28/2018	Update distribution lists and draft instructions for replacing Posting Amount objects with Jrnl Posting Amount.	
10/3/2018	Obtain Core Team approval for instructions	Core Team consists of eMARS managers
10/5/2018	Obtain Reporting Team approval for instructions	Reporting team consists of representatives from other functional areas and agencies
10/8/2018	Announce target date of 10/19/2018 to replace Posting Amount with Jrnl Posting Amt to Report Developers via email (with instructions attached)	Request notification from agencies if target date cannot be achieved
10/15/2018	Redesign Statewide Reports to use Jrnl Posting Amt instead of Posting Amount	
10/22/2018	Disable Basic Accounting Ledger and Detail Accounting Ledger classes	As part of CGI's baseline, also log ticket(s) and/or enhancement request(s) to try to prevent this change from remaining "custom"

FINANCIAL STATEMENT FINDINGS

Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 18-FAC-03: The Office Of Procurement Services Failed To Detect An Error Prior To Bid Closure

The Office of Procurement Services (OPS) acts as the central procurement agency for the Executive Branch and is responsible for purchasing all commodities and non-professional services for state agencies in excess of their small purchase authority. During fiscal year 2018, OPS posted a solicitation for the purchase of agency equipment. During the open bidding period, the purchasing agency requested the scope of the bid be expanded to include equipment made of different materials. A material change is defined as affecting price, quantity, quality, or delivery of the commodity, and requires a solicitation modification. Solicitation modifications should remain open for seven days after they are uploaded to the state's eProcurement website. Per discussions with OPS this change met the criteria for being material, and accordingly, OPS should have extended the bid opening period by an additional seven days, but only extended it by six days.

The wrong date was chosen by an employee when issuing the modification, and FAC's review process did not detect the error prior to bid closure.

A best value bidder could be excluded from a bid opening as result of a shortened time frame to respond to any material changes which may affect their bid. Excluding a best value bidder without providing appropriate time to respond to a bid opening is not in the financial best interest of the Commonwealth.

FAP 111-35-00, Competitive Sealed Bidding, states:

> 6. Minimum Times to be allowed for Bid Response:
> Solicitations and material modifications of the Solicitations shall be closed no sooner than seven (7) days after they are uploaded electronically to the state's eProcurement website. Solicitation modifications shall be provided adequate public notice of any change to a Solicitation and posted on the state's eProcurement website.

Recommendation

FAC implement quality control procedures in order to ensure compliance with established policies.

Management's Response and Planned Corrective Action

The Office of Procurement Services (OPS) acknowledges that human error resulted in a solicitation addendum failing to remain open seven (7) days as is required when making a material change to a solicitation. As an additional measure to the current review process, the OPS File Room Administrative Assistant will send a daily reminder to all OPS staff of the "Seventh Day from Today". The reminder will note if the seventh day is a holiday and advise staff to select a date after that date for any solicitation closings.

FINDING 18-FAC-03: The Office Of Procurement Services Failed To Detect An Error Prior To Bid Closure (Continued)

Management's Response and Planned Corrective Action (Continued)

OPS investigate adding a warning message to the eMARS system to alert a user when a closing date selected is not seven days from the current date. A change of this nature requires a "system enhancement", which would result in a charge to the Commonwealth. Since this error rarely occurs, OPS is implementing the aforementioned control procedure.

FINANCIAL STATEMENT FINDINGS

Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 18-FAC-04: The Finance And Administration Cabinet Did Not Ensure The Enhanced Management Administrative And Reporting System Was Properly Secured

Four users of the enhanced Management Administrative and Reporting System (eMARS) had unnecessary access to the system during FY 2018. Similar issues were noted in FY 2016, but there have been significant improvements.

There are five components of the eMARS security module – Resource Groups, Application Resources, Security Roles, Access Control, and User Administration. A Resource Group is a collection of application resources that have similar authorization requirements and are secured in the same way. An Application Resource is any item in eMARS, such as a table, document, query, or HTML page, to which security rules are applied. The collection of user roles with the same tasks and security requirements is known as a Security Role. Access Control dictates which Security Roles have access to which Resource Groups and the extent of that access. User Administration allows for the establishment of a unique identifier for each user, which enables the user to log on to the application and links the user to one or more Security Roles.

The majority of all eMARS users have been granted access to the INTERNAL Security Role since it contains certain "default" system settings such as page security (for all users) and row filtering for organizational security. This security role allows full update access to almost every table in the eMARS application. To ensure the access granted was appropriate, we performed testing on employees that had a user ID with an unconventional name, user IDs that appeared to be group accounts based on the naming convention, and individuals that appeared to have duplicate user IDs. This testing revealed four users had unnecessary access to eMARS during FY 2018 through duplicate accounts. Finance disabled the unnecessary duplicate accounts during fieldwork.

Various situations can occur which cause an individual to need a new user ID to be created. Finance did not ensure unnecessary duplicate accounts were disabled in all cases.

Without strong, formalized logical security controls, the opportunity increases for unauthorized modification to financial information and staffing reports as well as the likelihood of errors or losses occurring from incorrect use of data and other resources.

According to the eMARS Security and Workflow Plan, Resource Groups are created to which all Application Resources are assigned. Security Roles are defined for various user groups by their tasks and/or responsibilities. Security Roles and Resource Groups are mapped through Access Control to meet established security and authorization requirements. One of the primary requirements of any financial system is to maintain data integrity. System security is a critical aspect to maintaining data integrity in a system. System access must be limited to the level necessary for performing assigned duties.

FINANCIAL STATEMENT FINDINGS

Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 18-FAC-04: The Finance And Administration Cabinet Did Not Ensure The Enhanced Management Administrative And Reporting System Was Properly Secured (Continued)

Recommendation

We recommend Finance ensure any existing accounts for a user are disabled upon creating a new user ID for the user. In addition, we recommend Finance regularly review user accounts that have been granted access to the INTERNAL Security Role to ensure access is still necessary. Any actions taken by Finance should be documented and maintained for audit purposes.

Management's Response and Planned Corrective Action

Prior to creating a new user account Finance will ensure there are no active user accounts for the individual in the application. With the exception of the auditors in the APA Office the INTERNAL security role is one of the "default" security roles that are assigned to all users. It allows access to a number of "internal" tables that are impacted by the posting of documents and it controls access to Worklists, Workspaces, and other basic navigational aspects of the system that the user would need to have.

FINANCIAL STATEMENT FINDINGS

Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 18-OFM-01: The Office Of Financial Management Did Not Update And Consistently Apply Logical Security Procedures Related To The CAMRA Server And Production Library

The fiscal year (FY) 2018 audit of the Office of Financial Management (OFM) revealed the agency did not update or consistently apply logical security procedures. The agency has a formalized policy for requesting access to the CAMRA server and production library, which houses the OFM databases used in daily and monthly processing of the state's cash and investments. Although the policy had been updated, it does not reflect the current date of review or current procedures. In addition, it was not consistently followed.

According to the OFM CAMRA Server Access policy, any type of user access to the production library should be requested using an F181 form. This form should include the specific permissions requested. Once the access request is reviewed and approved, the F181 form should then be submitted in an email to the Commonwealth Office of Technology (COT) for processing. COT is responsible for physically granting, assigning, or removing access and user permissions to the OFM production library.

Testing of six new users revealed OFM does not clearly indicate permission levels to be given to individuals on the F181 forms. Five of the six new users had incorrect permission levels listed for the requested folders. Each of these individuals required 'Modify' access, but their forms indicated 'Read Only' in the 'Permission' field or this field was left blank. Specifically, the access for two users was incorrectly listed as 'Read Only', the field was left blank for two users, and the permission level was 'Read Only' for one folder and blank for the other folder for the remaining user. OFM indicated the users required 'Modify' access since cross-training of OFM employees is necessary to ensure work is completed with limited staff. OFM believes COT is aware of this situation and grants 'Modify' access to OFM employees unless the 'Comments' section of the F181 form states otherwise. However, for the sixth new user, although the form requested 'Read/Write' permissions, 'Read and Execute, Write' access was granted. OFM stated this was likely a difference in how the request was processed by COT. This situation was not reviewed by OFM to determine if the correct permissions were given. It should be noted this employee is no longer with OFM and their account has been disabled.

According to the OFM CAMRA Server Access policy, changes in access should follow the same process as new requests. Testing of one modified user account revealed no documentation was maintained to support the change in access from 'Full Control' to 'Modify'. All individuals involved with this change left OFM prior to the auditor's inquiry.

The OFM CAMRA Server Access policy states, upon termination, retirement, or departure of an OFM employee, an email must be sent to COT to request the removal of permissions. However, COT no longer requires an email due to the implementation of the Enterprise Identity Management (EIM) solution. Review of five individuals who are no longer with OFM revealed the agency sent an email to COT for three of the individuals.

FINANCIAL STATEMENT FINDINGS

Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 18-OFM-01: The Office Of Financial Management Did Not Update And Consistently Apply Logical Security Procedures Related To The CAMRA Server And Production Library (Continued)

The OFM CAMRA Server Access policy requires OFM conduct an annual review of server groups to ensure all access is appropriate. Although OFM conducted this review during the calendar year (CY) 2017, it was not completed until the auditor's request for a user listing. OFM confirmed they were unaware the annual review was not completed until this request was made.

OFM management did not ensure the formalized procedures were updated or consistently followed and that all documentation was centrally maintained. Significant turnover at the agency is a possible cause of this situation.

Failure to consistently apply logical security controls could result in an increased risk for unauthorized access, unintended or malicious modification to computer programs and data, destruction of assets, a failure to comply with security policies, failure to perform assigned security responsibilities, or inappropriate and inefficient use of system resources. Allowing users unnecessary access may subject the processing of data to errors and/or omissions and may compromise the integrity of data processed through the production library.

Logical security controls must be finalized, approved, thoroughly documented, and consistently applied to ensure only authorized individuals are allowed access to a system. All authorized requestors should be provided with the most recent versions of forms and procedures to ensure the approved procedures are being followed. All requests for access or privileges to a system should be properly authorized, reviewed, and documented.

According to the National Institute of Standards and Technology (NIST) Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, an organization should employ "the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions." NIST 800-53 also acknowledges that certain assigned user privileges may change over time, reflecting changes in organizational missions/business function, environments of operation, technologies, or threat. Therefore, "periodic review of assigned user privileges is necessary to determine if the rationale for assigning such privileges remains valid. If the need cannot be revalidated, organizations take appropriate corrective actions."

FINANCIAL STATEMENT FINDINGS

Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 18-OFM-01: The Office Of Financial Management Did Not Update And Consistently Apply Logical Security Procedures Related To The CAMRA Server And Production Library (Continued)

Further, according to the CAMRA Server Access policy:

> "Access or change to the 'CAMRA' server (CAMRA data, Batchjob library and CAMRA data storage) must be reviewed and approved by the OFM Accounting Manager. After approval and if applicable a support ticket or email must be submitted by an employee of the Office of Financial Management ('OFM') to the Commonwealth Office of Technology ('COT') Commonwealth Service Desk Team requesting the necessary permission changes or additions to the appropriate Server Group(s).
>
> Upon addition of an OFM employee, the addition of permissions to the ... server will be part of the initial F181 COT request to add the user.
>
> Upon termination, retirement, or departure of an OFM employee the removal of permissions to the… server will be communicated via email to COT in a timely manner.
>
> Server Group(s) will be reviewed annually by an employee of OFM…"

Recommendation

We recommend OFM review and update their formal access policy to ensure it reflects the actual procedures OFM personnel should follow regarding submitting new, change, and termination of access requests, as well as reviewing user access, related to the OFM CAMRA server and production library. Specifically, OFM should ensure the policy fully explains the process for reviewing the server groups annually. This may include the need to conduct the review in a certain month, to centrally maintain a log of the reviews, and to centrally maintain all documentation and correspondence related to the reviews. In addition, OFM should determine if the email to COT is necessary when an individual terminates employment. The policy should be updated accordingly and the chosen process should be consistently followed. Once the formal access policy has been decided, the revision date should be updated on the document and it should be distributed to all OFM personnel with responsibilities within this process. Additionally, OFM management should ensure applicable staff are properly trained and held accountable to the formal logical security procedures.

Furthermore, OFM should clearly state the permission levels requested on the F181 form. The documentation for all changes in user access should be centrally maintained for management and audit purposes.

FINANCIAL STATEMENT FINDINGS

Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 18-OFM-01: The Office Of Financial Management Did Not Update And Consistently Apply Logical Security Procedures Related To The CAMRA Server And Production Library (Continued)

Management's Response and Planned Corrective Action

In response to the CAMRA Server Access Policy:
OFM has reviewed and updated in more detail procedures for CAMRA server access. Additionally the policy defines the process for reviewing the server groups for accuracy during the year-end processing, timeliness of correcting issues and notification for employees leaving OFM.

In response to the F181 forms:
OFM has created a central folder on the common share drive for all COT forms. We will make draft forms for the positions in the office to eliminate confusion on the required servers and permissions. Two staff members (Accounting Manager and Office Coordinator) will take COT's course on EIM for ticket submission.

Auditor's Note

OFM provided the updated Procedures for CAMRA Server Access discussed above.