STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2020-056
November 2019

DEPARTMENT OF FINANCIAL SERVICES

Division of Treasury
Selected Treasury Systems

Sherrill F. Norman, CPA
Auditor General

Chief Financial Officer

Pursuant to Article IV, Sections 4(c) and 5(a) of the State Constitution, the Chief Financial Officer is an elected member of the Cabinet and serves as the chief fiscal officer of the State. Pursuant to Section 20.121(1), Florida Statutes, the Chief Financial Officer is the head of the Department of Financial Services. The Honorable Jimmy Patronis served as Chief Financial Officer during the period of our audit.

The audit was supervised by Hilda S. Morgan, CPA, CISA.

Please address inquiries regarding this report to Brenda Shiner, CISA, Audit Manager, by e-mail at brendashiner@aud.state.fl.us or by telephone at (850) 412-2946.

This report and other reports prepared by the Auditor General are available at:

FLAuditor.gov

Printed copies of our reports may be requested by contacting us at:

State of Florida Auditor General
Claude Pepper Building, Suite G74 • 111 West Madison Street • Tallahassee, FL 32399-1450 • (850) 412-2722

DEPARTMENT OF FINANCIAL SERVICES

Division of Treasury
Selected Treasury Systems

SUMMARY

This operational audit of the Department of Financial Services (Department), Division of Treasury (Division), focused on evaluating selected information technology (IT) controls applicable to the integrated Cash Management Subsystem (CMS), Investment Accounting System (IAS), and Bank Accounts application (Bank Accounts) and included a follow-up on the findings in our report No. 2015-096. Our audit disclosed the following:

Finding 1: Some access controls related to CMS and Bank Accounts user access privileges continue to need improvement to promote an appropriate separation of duties and restrict users to only those functions necessary for their assigned job responsibilities.

Finding 2: Department procedures need improvement to ensure that periodic reviews are conducted of all user accounts, including all administrative accounts, on the Department's network domain, CMS servers and databases, and IAS and Bank Accounts servers, databases, and production libraries.

Finding 3: The Division did not timely disable the CMS access privileges of a former employee or the IAS and Bank Accounts access privileges of two transferred employees and one former employee.

Finding 4: Department change management controls need improvement to ensure that only authorized, tested, and approved CMS and Bank Accounts program changes are implemented into the production environment. Similar findings related to the reconciliations were noted in prior audits of the Department.

Finding 5: Department backup controls need improvement to incorporate periodic restoration testing from the backup media for the CMS, IAS, and Bank Accounts.

Finding 6: Certain security controls related to logical access, user authentication, and logging and monitoring continue to need improvement to help ensure the confidentiality, integrity, and availability of CMS, IAS, and Bank Accounts data and related IT resources.

BACKGROUND

The Chief Financial Officer (CFO) is the head of the Department of Financial Services (Department) and, as the chief fiscal officer of the State, is responsible for settling and approving accounts against the State and keeping all State funds and securities. The CFO is designated the cash management officer for the State and is charged with the coordination and supervision of procedures providing for the efficient handling of financial assets under the control of the Division of Treasury (Division), State agencies, and the judicial branch. The Division receives and disburses cash, invests available balances, and performs related accounting functions, cash management operations, and consultations**.**

Pursuant to State law,[1] the CFO is the functional owner of the Cash Management Subsystem (CMS), a subsystem of the Florida Financial Management Information System, and requires that the CMS include functions for recording and reconciling credits and debits to State Treasury fund accounts, monitoring cash levels and activities in State bank accounts, monitoring short-term investments of idle cash, and administering the provisions of the Federal Cash Management Improvement Act of 1990. To carry out its responsibilities, the Division operates three integrated and ten nonintegrated legacy business applications that collectively compose the CMS.[2]

Our audit focused on the integrated portion of the CMS, which assimilated processing, verifying, and storing agency deposit and returned item details and reconciling the bank account ledgers, and the legacy Investment Accounting System (IAS) and Bank Accounts application (Bank Accounts). The IAS is used to account for all investments made by the Treasury internal and external portfolios and includes interest amounts to be allocated. Bank Accounts is used to account for all Treasury assets including bank account balances and investment transactions. In 2018, the Department executed a contract to design, build, and implement the Florida Planning, Accounting, and Ledger Management (PALM) Solution, an integrated, enterprise financial management solution, to replace the State's accounting system, Florida Accounting Information Resource Subsystem (FLAIR), and the CMS.

FINDINGS AND RECOMMENDATIONS

Finding 1: Appropriateness of Access Privileges

Effective access controls include measures that limit users' access privileges to only those system functions necessary to perform their assigned job duties and promote an appropriate separation of duties. Agency for State Technology (AST)[3] rules[4] required each agency to ensure that access permissions are managed, incorporating the principles of least privilege and separation of duties. Our audit procedures disclosed that some unnecessary or incompatible access privileges existed for the CMS and Bank Accounts. Specifically, we evaluated the access privileges for the 20 CMS internal users assigned update access privileges and the 9 users assigned update access privileges to Bank Accounts and found that:

- 1 security administrator and 1 end-user were assigned incompatible CMS access roles by combining security administration with end-user access roles, contrary to an appropriate separation of duties. Another security administrator and an Office of Information Technology (OIT) employee were assigned unnecessary end-user access roles that resulted in a combination of incompatible access privileges. We also found that 2 CMS users were assigned end-user

[1] Section 215.94(3), Florida Statutes.

[2] CMS includes the integrated applications Verifies, Receipts, Chargebacks; and the legacy applications Fund Accounting, Bank Accounts, State Accounts, Dis-Investments, Investment Accounting System, Certificates of Deposit, Consolidated Revolving Account, Special Purpose Investment Accounts, Archive, and Warrant Processing.

[3] Effective July 1, 2019, Chapter 2019-118, Laws of Florida, creates the Division of State Technology within the Department of Management Services (DMS) and transfers the existing powers, duties, functions, personnel, records, property, and funds of the AST to the Division of State Technology.

[4] AST Rule 74-2.003(1)(d), Florida Administrative Code. Effective July 1, 2019, AST Rules, Chapter 74-2, Florida Administrative Code, was transferred to the DMS Rules, Chapter 60GG-2, Florida Administrative Code. AST Rules, Chapter 74-2, Florida Administrative Code, was in effect during our audit period (July 2018 through March 2019).

access roles that were unnecessary for the users' assigned job responsibilities. A similar finding was noted in our report No. 2015-096.

- 2 users had update access privileges to Bank Accounts that were unnecessary for the users' assigned job responsibilities.

Appropriately restricted access privileges help protect data and IT resources from unauthorized modification, loss, or disclosure.

Recommendation: We recommend that Division management limit user access privileges to the CMS and Bank Accounts to promote an appropriate separation of duties and restrict users to only those functions necessary for the users' assigned job responsibilities.

Finding 2: Periodic Review of Access Privileges

AST rules[5] required agency information owners to review access rights (privileges) periodically based on system categorization or assessed risk. Periodic reviews of user access privileges help ensure that only authorized users have access and that the access privileges provided to each user remains appropriate. An effective periodic review consists of identifying the current access privileges of all system users and evaluating the assigned access privileges to ensure that they align with the users' job responsibilities. Department policy[6] requires a formal process for the periodic review and confirmation of user accounts, access controls, and privileges.

Our audit procedures disclosed that the Department's periodic review procedures need improvement. Specifically, we found that:

- The Department had not performed a periodic review of the administrative accounts used to manage the Department's network domain and the CMS servers as of January 28, 2019, and the CMS database as of March 6, 2019. In response to our audit inquiry, Department management within Mid Range Systems of the Bureau of Distributed Infrastructure stated that they did not deem reviews of the administrative accounts for the network domain and the CMS servers necessary.
- While the Information Security Office received quarterly reports listing user and administrative access privileges for the IAS and Bank Accounts servers, databases, and production libraries for review purposes, Department records did not evidence that reviews were performed during the period July 2018 through January 2019. In response to our audit inquiry, Department management indicated that, due to staff changes in the Information Security Office during December 2018, records of the prior reviews were not available.

Conducting periodic reviews of all user accounts, including all administrative accounts, helps ensure that only authorized users have access and that the access privileges provided to each user remain appropriate.

Recommendation: We recommend that Department management ensure that periodic reviews of all user accounts, including all administrative accounts on the Department's network domain; CMS servers and databases; and IAS and Bank Accounts servers, databases, and production libraries are conducted, and that documentation of such reviews is maintained.

[5] AST Rule 74-2.003(1)(a)6., Florida Administrative Code.

[6] Administrative Policies and Procedures, *Information Technology Security Policy*, No. 4-03.

Finding 3: Timely Disabled User Accounts

AST rules[7] required agency control measures that ensure IT access is removed when an IT resource is no longer required. Prompt action to disable access privileges when a user separates from employment or access to the information is no longer required is necessary to help prevent the misuse of the access privileges. Our review of logical access privileges to the CMS, IAS, and Bank Accounts found instances where access privileges were not timely disabled for former or transferred employees. Specifically:

- We compared the list of employees who separated from Division employment during the period July 1, 2017, through December 10, 2018, to the list of CMS active and disabled user accounts as of December 10, 2018, to determine whether CMS access privileges were timely disabled. For one of the four former Division employees who had access to the CMS, the assigned user account was not disabled until 24 days after the former employee separated from Division employment.
- Due to system limitations, the Division was unable to provide a system-generated list of disabled IAS and Bank Accounts user accounts. Therefore, we requested the Division to identify former and transferred employees from the list of employees who separated from Division employment or transferred to other positions during the period July 1, 2017, through December 15, 2018, who were previously assigned IAS or Bank Accounts user accounts and the dates the users' access privileges were disabled. We then compared the dates of employment separation or transfer to the dates the respective employees' access privileges were disabled as reported by Division management. We found that, for two transferred employees, access privileges were not timely disabled. One employee's IAS and Bank Accounts access privileges were disabled 5 days after the employee's transfer and the other employee's Bank Accounts access privileges were disabled 13 days after the employee's transfer. Through additional audit procedures we identified one active user account with access privileges to the production libraries as of November 27, 2018, that was assigned to a former employee who separated from Department employment on March 13, 2015.

Timely disabled application user accounts upon an employee's separation from Division employment or position transfer reduces the risk that the application access privileges may be misused by the former employee or others.

Recommendation: We recommend that Division management ensure that CMS, IAS, and Bank Accounts user access privileges are timely disabled upon a user's separation from Department employment or transfer to another position where access is no longer needed.

Finding 4: Change Management Controls

Effective change management controls are intended to ensure that all program modifications are properly authorized, tested, and approved for implementation into the production environment. Effective change management controls also incorporate the conduct of reconciliations to ensure that the established change management process is followed when the program changes are implemented into the production environment.

We selected the five production program changes made to the CMS and the one production program change made to Bank Accounts during the period July 1, 2017, through December 13, 2018, to evaluate whether the program changes implemented into the production environment appropriately followed the

[7] AST Rule 74-2.003(1)(a)8., Florida Administrative Code.

Department's change management process. Our audit procedures disclosed that the Department's change management controls need improvement. Specifically, we found that documentation was not always maintained, or available documentation did not contain sufficient information, to demonstrate that:

- Two of the CMS program changes and the one Bank Accounts program change were appropriately authorized by OIT staff.
- One of the CMS program changes was appropriately tested by the Division.
- Two of the CMS program changes and the one Bank Accounts program change were appropriately approved by the OIT before being implemented into the production environment.

We also found that, while the Department used a change management system for managing program changes, the Department did not have a mechanism in place to detect and reconcile all IAS and Bank Accounts program changes moved into the production environments to the change management system. As a result, Department management could not verify that all IAS and Bank Accounts program changes were managed by, and did not bypass, the Department's change management system. Similar findings were noted in prior audits of the Department, most recently in our report No. 2015-096.

Effective change management controls, including appropriate documentation and reconciliations, provide assurance that all program changes have followed the Department's change management process and that all program changes moved into the production environment have been appropriately authorized, tested, and approved and did not bypass the change management system.

Recommendation: We recommend that Department management retain documentation to demonstrate that only authorized, tested, and approved CMS and Bank Accounts program changes are implemented into the production environment. We also recommend that reconciliations be performed to verify that all implemented IAS and Bank Accounts program changes were managed by, and did not bypass, the Department's change management system.

Finding 5: Backup Controls

Effective backup controls include policies and procedures that provide guidance for an entity's backup processes, including identification of the IT resources requiring back up, the frequency of backups, and the periodic restoration testing for recoverability to prevent or minimize the damage to automated operations that can occur from unexpected events. Effective backup management controls include a backup and restore strategy that incorporates periodic restoration testing from the backup media. AST rules[8] required each agency to develop procedures to prevent loss of data and to ensure that backups of information are conducted, maintained, and tested.

Our audit procedures disclosed that Division backup controls for the CMS, IAS, and Bank Accounts need improvement. Specifically, the Division had not established policies and procedures to define the frequency of periodic restoration testing from the backup media for the CMS, IAS, and Bank Accounts to validate that the backups are intact and can be used to meet recoverability objectives. Our audit procedures disclosed that the Department did not perform periodic restoration testing of the CMS, IAS, and Bank Accounts backup media to validate the backups were sufficient for recoverability. In response to our audit inquiry, Department management indicated that the OIT does not perform periodic restoration

[8] AST Rules 74-2.003(5)(d) and 74-2.006(1)(c), Florida Administrative Code.

testing to validate backup media and that Division management would need to organize and schedule backup media restoration testing as required by AST rules.

Periodic restoration testing to validate selected backups helps provide assurance that data is readily recoverable from the backup media when needed in response to an unexpected event and that data will be timely and completely recoverable in the event of a loss of production data.

Recommendation: We recommend that Division management establish policies and procedures to define the frequency of periodic restoration testing of the backup media for the CMS, IAS, and Bank Accounts, and ensure that periodic restoration testing from the backup media is performed to validate that the backups are intact and can be used to meet recoverability objectives.

Finding 6: Security Controls – Logical Access, User Authentication, and Logging and Monitoring

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit procedures disclosed that certain security controls related to logical access, user authentication, and logging and monitoring need improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising Department data and IT resources. However, we have notified appropriate management of the specific issues. Similar findings were communicated to Department management in connection with prior audits of the Department, most recently with our report No. 2015-096.

Without adequate security controls related to logical access, user authentication, and logging and monitoring, the risk is increased that the confidentiality, integrity, and availability of Department data and related IT resources may be compromised.

Recommendation: We recommend that Department management improve certain security controls related to logical access, user authentication, and logging and monitoring to ensure the confidentiality, integrity, and availability of Department data and related IT resources.

PRIOR AUDIT FOLLOW-UP

Except as discussed in the preceding paragraphs, the Department had taken corrective actions for the findings included in our report No. 2015-096.

OBJECTIVES, SCOPE, AND METHODOLOGY

The Auditor General conducts operational audits of governmental entities to provide the Legislature, Florida's citizens, public entity management, and other stakeholders unbiased, timely, and relevant information for use in promoting government accountability and stewardship and improving government operations.

We conducted this information technology (IT) operational audit from October 2018 through May 2019 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 the audit findings and our conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for the audit findings and our conclusions based on our audit objectives.

This IT operational audit focused on evaluating selected Department of Financial Services (Department) IT business process application controls and application-level general controls for selected Treasury systems during the period July 2018 through March 2019 and selected actions subsequent thereto. The overall objectives of the audit were:

- To determine the effectiveness of selected IT controls in achieving management's control objectives in the categories of compliance with controlling laws, administrative rules, and other guidelines; the confidentiality, integrity, availability, relevance, and reliability of data; and the safeguarding of IT resources.
- To determine whether management had corrected, or was in the process of correcting, all deficiencies disclosed in our report No. 2015-096.
- To identify statutory and fiscal changes that may be recommended to the Legislature pursuant to Section 11.45(7)(h), Florida Statutes.

This audit was designed to identify, for the IT systems and controls included within the scope of the audit, deficiencies in management's internal controls; instances of noncompliance with applicable governing laws, rules, or contracts; and instances of inefficient or ineffective operational policies, procedures, or practices. The focus of this audit was to identify problems so that they may be corrected in such a way as to improve government accountability and efficiency and the stewardship of management. Professional judgment has been used in determining significance and audit risk and in selecting the particular IT controls, legal compliance matters, and records considered.

As described in more detail below, for the IT systems and controls included within the scope of this audit, our audit work included, but was not limited to, communicating to management and those charged with governance the scope, objectives, timing, overall methodology, and reporting of the audit; obtaining an understanding of the IT systems and controls; exercising professional judgment in considering significance and audit risk in the design and execution of the research, interviews, tests, analyses, and other procedures included in the audit methodology; obtaining reasonable assurance of the overall sufficiency and appropriateness of the evidence gathered in support of the audit findings and our conclusions; and reporting on the results of the audit as required by governing laws and auditing standards.

This audit included the selection and examination of IT system controls and records. Unless otherwise indicated in this report, these items were not selected with the intent of statistically projecting the results, although we have presented for perspective, where practicable, information concerning relevant population value or size and quantifications relative to the items selected for examination.

An audit by its nature does not include a review of all records and actions of agency management, staff, and contractors and, as a consequence, cannot be relied upon to identify all instances of noncompliance, fraud, abuse, or inefficiency.

In conducting this audit, we:

- Interviewed Department personnel and reviewed Department and Division of Treasury (Division) documentation to obtain an understanding of:

  - The Cash Management Subsystem (CMS), Investment Accounting System (IAS), and Bank Accounts application (Bank Accounts) computing platform and logical access processes including hardware, software, operating system, and security software for the applications and databases.
  - Backup processes utilized for the production libraries and databases supporting the CMS, IAS, and Bank Accounts.
  - Logical access controls for administrative accounts on the production servers supporting the CMS, IAS, and Bank Accounts.
  - Key processes and tools for implementing program and data changes for the CMS, IAS, and Bank Accounts.
  - Logical application access controls for the CMS, IAS, and Bank Accounts including periodic reviews.
  - The purpose of the CMS, IAS, and Bank Accounts, including data flows, and interfaces among the CMS, IAS, and Bank Accounts and the Central Accounting Component in the Florida Accounting Information Resource Subsystem (FLAIR).
- Evaluated logical access controls for administrative accounts for the network, CMS, IAS, and Bank Accounts IT resources including periodic access reviews. Specifically, we evaluated:
  - Department procedures and examined Department records to determine whether periodic reviews were performed to evaluate the appropriateness of administrative access privileges used to manage the Department's network domain, the CMS servers and databases, and the IAS and Bank Accounts servers, databases, and production libraries.
  - The effectiveness of logical access controls as of November 27 and December 14, 2018, for network accounts with administrative access privileges on the Department's network.
  - The object authorities assigned to 45 active user profiles with access privileges to the IAS and Bank Accounts production libraries and the public authority settings for the IAS and Bank Accounts production libraries, containing the program and database files, as of November 27, 2018, to determine whether the access privileges were appropriate.
  - The access members and permissions for the CMS object code location as of December 12, 2018, and for the implementation configuration for the deployment application that implements the CMS object code as of February 5, 2019, to determine whether the access privileges to the CMS object code were appropriate.
  - The 14 CMS database accounts as of December 3, 2018, to determine whether the access privileges to the CMS database were appropriate.
  - The 21 CMS accounts with administrative privileges for managing the CMS database as of December 17, 2018, to determine whether the access privileges were appropriate.
  - The 27 user accounts as of January 16, 2019, for the CMS, and the 8 user accounts as of January 31, 2019, for the IAS and Bank Accounts in the source management system to determine whether the access privileges to update program source code for the CMS, IAS, and Bank Accounts were appropriate.
  - The 17 user accounts (excluding accounts in the *Domain Admins* security group) as of November 27 and December 3, 2018, with access privileges in the local *Administrators* security groups on the nine CMS production servers to determine whether the administrative access privileges were appropriate for the user accounts.
  - The 43 service accounts as of November 27 and December 3, 2018, dispersed within the local *Administrators* security groups on the nine CMS production servers, and 9 of the 16 service accounts as of November 27 and December 4, 2018, included in two Active

  - Directory security groups (excluding accounts in the *Domain Admins* security group) that were added locally to one CMS application server and six CMS database servers to determine whether the administrative access privileges were appropriate for the services associated with the service accounts.
  - The 33 servers and one service account with local administrator access on the six CMS database servers as of December 4, 2018, to determine whether the administrative access privileges were appropriate.
  - The 80 service accounts with administrative access privileges to determine whether appropriate policies were applied to prevent the service accounts from being used to anonymously log on locally or remotely as an administrator.
- Evaluated the adequacy of logging and monitoring controls for the CMS, IAS, and Bank Accounts applications and related databases.
- Reviewed backup and recovery policies and procedures for the CMS, IAS, and Bank Accounts applications and databases, selected logs of the backups conducted, and documentation of recoverability testing.
- Evaluated the adequacy of identification and authentication controls including policies and procedures and authentication settings for the CMS, IAS, and Bank Accounts applications, databases, and production servers and a deployment server. Specifically, we evaluated:
  - The authentication settings as of December 7 and December 14, 2018, for the CMS production servers; November 27, 2018, for the IAS, and Bank Accounts production servers; and March 8, 2019, for the three CMS application servers and a deployment server.
  - The authentication settings as of November 27, 2018, for the internal CMS users, and December 06, 2018, for the external CMS users, and the authentication settings as of November 27, 2018, for the IAS and Bank Accounts users.
  - The authentication settings as of November 27, 2018, for the CMS, IAS, and Bank Accounts databases.
- Evaluated Department procedures and selected program and data change management controls for the CMS, IAS, and Bank Accounts. Specifically, we evaluated the effectiveness of change management controls for:
  - The five CMS and the one Bank Accounts closed program changes that were requested during the period of July 1, 2017, through December 13, 2018, to ensure the appropriateness of authorization, testing, approval for production, and implementation into the production environment.
  - 9 of 21 CMS and 6 of 12 IAS closed data changes that were requested during the period of July 1, 2017, through December 13, 2018, to ensure the appropriateness of authorization prior to implementation into the production environment.
- Evaluated the appropriateness of all active users as of November 19, 2018, with access privileges to the CMS, IAS, and Bank Accounts to determine whether the access was appropriate based on the user's job function. Specifically, we evaluated:
  - The 20 active internal users with update access privileges to the CMS to determine whether the access was appropriate based on the user's job function.
  - The 7 active users with update access privileges to the IAS to determine whether the access was appropriate based on the user's job function.
  - The 9 active users with update access privileges to Bank Accounts to determine whether the access was appropriate based on the user's job function.

- Evaluated Department records as of December 4, 2018, to determine whether action was taken to remediate a prior audit finding related to read-only access for the internal auditor role in CMS.
- Evaluated the access privileges as of December 10, 2018, to determine whether the access privileges to the CMS, IAS, and Bank Accounts were periodically reviewed and timely removed. Specifically, we:
  - Examined Division records of the September, October, and November 2018 user access reviews conducted of the CMS internal user accounts and the IAS and Bank Accounts user accounts and examined a CMS external user report as of December 10, 2018, to determine the adequacy of the quarterly external access reviews conducted.
  - Compared the names of two former OIT employees to the list of CMS active and inactive user accounts to determine whether the CMS access privileges of former OIT employees who had previously been granted CMS application user accounts were timely removed.
  - Evaluated the CMS user accounts of the four former employees who separated from Division employment during the period July 1, 2017, through December 10, 2018, and were on the CMS active and inactive user accounts list as of December 10, 2018, to determine whether CMS access privileges were timely removed.
  - Reviewed the manual records of disabled accounts for the three IAS and Bank Accounts users who separated or transferred from Division employment during the period July 1, 2017, through December 15, 2018, and who were previously assigned IAS or Bank Accounts user accounts, to determine whether the IAS and Bank Accounts access privileges were timely removed.
- Evaluated the adequacy of interface processing procedures, reconciliations, and error handling processes related to interfaces among the CMS, IAS, and Bank Accounts and the Central Accounting Component in FLAIR.
- Communicated on an interim basis with applicable officials to ensure the timely resolution of issues involving controls and noncompliance.
- Performed various other auditing procedures, including analytical procedures, as necessary, to accomplish the objectives of the audit.
- Prepared and submitted for management response the findings and recommendations that are included in this report and which describe the matters requiring corrective actions. Management's response is included in this report under the heading ***MANAGEMENT'S RESPONSE***.

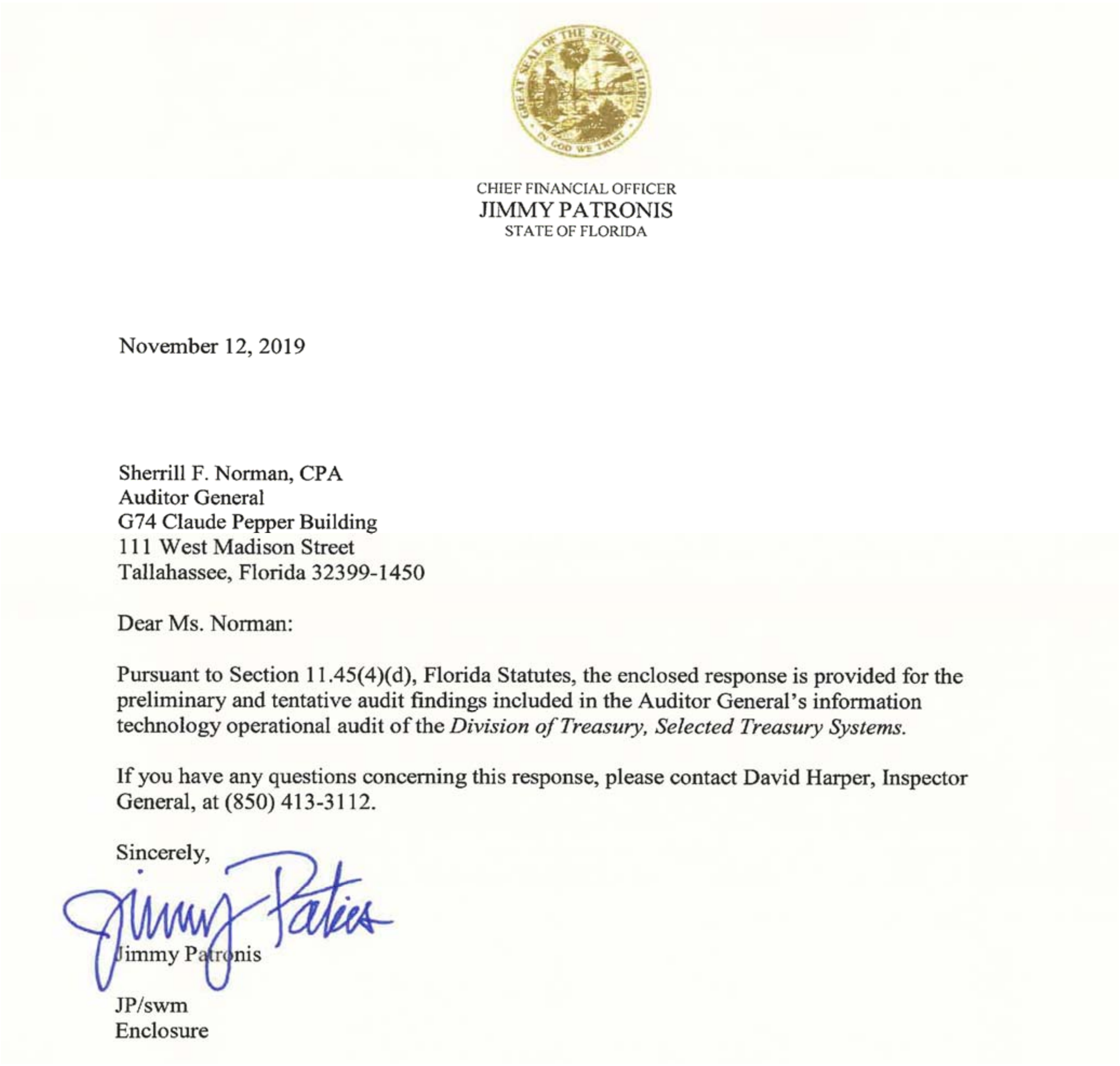
AUTHORITY

Section 11.45, Florida Statutes, provides that the Auditor General may conduct audits of the IT programs, activities, functions, or systems of any governmental entity created or established by law. Pursuant to the provisions of Section 11.45, Florida Statutes, I have directed that this report be prepared to present the results of our IT operational audit.

Sherrill F. Norman

Sherrill F. Norman, CPA
Auditor General

MANAGEMENT'S RESPONSE



CHIEF FINANCIAL OFFICER
JIMMY PATRONIS
STATE OF FLORIDA

November 12, 2019

Sherrill F. Norman, CPA
Auditor General
G74 Claude Pepper Building
111 West Madison Street
Tallahassee, Florida 32399-1450

Dear Ms. Norman:

Pursuant to Section 11.45(4)(d), Florida Statutes, the enclosed response is provided for the preliminary and tentative audit findings included in the Auditor General's information technology operational audit of the *Division of Treasury, Selected Treasury Systems.*

If you have any questions concerning this response, please contact David Harper, Inspector General, at (850) 413-3112.

Sincerely,

Jimmy Patronis

JP/swm
Enclosure

DEPARTMENT OF FINANCIAL SERVICES' RESPONSE TO PRELIMINARY AND TENTATIVE AUDIT FINDINGS

Finding No. 1: Appropriateness of Access Privileges

Some access controls related to CMS and Bank Accounts user access privileges continue to need improvement to promote an appropriate separation of duties and restrict users to only those functions necessary for their assigned job responsibilities.

Recommendation: We recommend that Division management limit user access privileges to the CMS and Bank Accounts to promote an appropriate separation of duties and restrict users to only those functions necessary for the users' assigned job responsibilities.

Response: We concur. The Department will review and modify access privileges for the user accesses identified as needing improvement. This is a moderate risk since the incompatible roles used by a small, identifiable group of users could create an opportunity for inappropriate use.

Expected Completion Date for Corrective Action: May 29, 2020

Finding No. 2: Periodic Review of Access Privileges

Department procedures need improvement to ensure that periodic reviews are conducted of all user accounts, including all administrative accounts, on the Department's network domain, CMS servers and databases, and IAS and Bank Accounts servers, databases, and production libraries.

Recommendation: We recommend that Department management ensure that periodic reviews of all user accounts, including all administrative accounts on the Department's network domain; CMS servers and databases; and IAS and Bank Accounts servers, databases, and production libraries are conducted, and that documentation of such reviews is maintained.

Response: We concur. This is a moderate risk. The Department is reviewing and revising all OIT policies and procedures, including the access control review process, to ensure they are current and adhered to by staff to address the concerns listed within this finding recommendation.

Expected Completion Date for Corrective Action: October 30, 2020

Finding No. 3: Timely Disabled User Accounts

The Division did not timely disable the CMS access privileges of a former employee or the IAS and Bank Accounts access privileges of two transferred employees and one former employee.

Recommendation: We recommend that Division management ensure that CMS, IAS, and Bank Accounts user access privileges are timely disabled upon a user's separation from Department employment or transfer to another position where access is no longer needed.

Response: We concur. The Department will continue to monitor access to the CMS, IAS, and Bank Accounts systems to ensure access is timely disabled.

Expected Completion Date for Corrective Action: Ongoing

Finding No. 4: Change Management Controls

Department change management controls need improvement to ensure that only authorized, tested, and approved CMS and Bank Accounts program changes are implemented into the production environment. Similar findings related to the reconciliations were noted in prior audits of the Department.

Recommendation: We recommend that Department management retain documentation to demonstrate that only authorized, tested, and approved CMS and Bank Accounts program changes are implemented into the production environment. We also recommend that reconciliations be performed to verify that all implemented IAS and Bank Accounts program changes were managed by, and did not bypass, the Department's change management system.

Response: Although we agree that documentation is not available, two of the CMS program changes and the one Bank Accounts program changes were appropriately authorized by OIT staff and approved prior to implementation into the production environment and the one CMS program change was appropriately tested by the Division. The change management system, according to the vendor, has known limitations for audit logging, making some approval information appear deficient. Some other approvals, due to a migration of the change management system during the review period, were lost. The Department will develop a process to ensure appropriate documentation is retained and changes are reconciled.

Expected Completion Date for Corrective Action: October 30, 2020

Finding No. 5: Backup Controls

Department backup controls need improvement to incorporate periodic restoration testing from the backup media for the CMS, IAS, and Bank Accounts.

Recommendation: We recommend that Division management establish policies and procedures to define the frequency of periodic restoration testing of the backup media for the CMS, IAS, and Bank Accounts, and ensure that periodic restoration testing from the backup media is performed to validate that the backups are intact and can be used to meet recoverability objectives.

Response: The Division will establish a policy and procedure framework to define the frequency of periodic restoration testing of the backup media for the CMS, IAS and Bank Accounts.

For IAS and Bank Accounts application, OIT agrees to ensure that periodic restoration testing from the backup media is performed to validate that the backups are intact and can be used to meet recoverability objectives.

Because of the maturity of CMS, the Department believes that periodic restoration testing cannot be conducted on the production environment due to the associated high risks for data corruption. The Department also currently lacks the resources to develop a new environment for such restoration testing. Additionally, the Cash Management System will be replaced in July 2021 with the launch of Florida PALM. The Department will ensure appropriate periodic restoration testing from backup media is performed within Florida PALM for the existing CMS functionality when the new system goes live.

Expected Completion Date for Corrective Action: October 30, 2020 and July 31, 2021

Finding No. 6: Security Controls – Logical Access, User Authentication, and Logging and Monitoring

Certain security controls related to logical access, user authentication, and logging and monitoring continue to need improvement to help ensure the confidentiality, integrity, and availability of CMS, IAS, and Bank Accounts data and related IT resources.

Recommendation: We recommend that Department management improve certain security controls related to logical access, user authentication, and logging and monitoring to ensure the confidentiality, integrity, and availability of Department data and related IT resources.

Response: The risk is moderate. As a result, OIT has performed some corrective actions to improve certain security controls related to logical access, user authentication, and logging and monitoring.

Expected Completion Date for Corrective Action: October 30, 2020