



September 24, 2019

MEMORANDUM

TO: Jim Zingale, Executive Director

FROM: Sharon Doredant, Inspector General

SUBJECT: Six-Month Update on Auditor General (AG) Report No. 2019-186, *State of Florida Compliance and Internal Controls Over Financial Reporting and Federal Awards*

As required by section 20.055(6)(h), *Florida Statutes*, this is the six-month update of corrective actions taken in response to AG Report No. 2019-186, *State of Florida Compliance and Internal Controls Over Financial Reporting and Federal Awards* for the fiscal year ended June 30, 2018.

AG Report No. 2019-186 contained one financial finding (Finding No. AM 2018-01): "The FDOR understated Receivables, net and Unavailable revenue due to an error in the preparation of year-end accrual entries."

STATUS: The Office of Financial Management asserted it has implemented an additional level of management review and associated training to ensure proper preparation of year-end accrual entries. The results of the current AG Financial Reporting Audit will determine if actions taken are effective and the finding can be closed.

In addition, AG Report No. 2019-186 (Finding No. 2018-016) incorporated by reference the findings previously reported in AG Report No. 2019-124, *Department of Revenue System for Unified Taxation (SUNTAX) Information Technology Operational Audit*. Three findings cited deficiencies related to access privileges. A fourth finding cited deficiencies related to logical access, user authentication, and logging and monitoring.

STATUS: As previously reported on August 13 in the SUNTAX audit update, the Information Services Program and the General Tax Administration Program are correcting these findings, with planned completion dates no later than November 2019. For specific details, see the attached six-month updates associated with AG Report No. 2019-124.

We did not verify the efficiency and effectiveness of corrective actions to address the problems identified by the external auditor. Additionally, we did not perform substantive

testing of system changes and changes that would require testing such as is performed in an audit.

If you have any questions, please contact me at 617-8152, or Marie Walker at 717-7598.

SD/mw

Attachments

cc: Andrea Moreland, Deputy Executive Director
Clark Rogers, Interim Chief of Staff
Damu Kuttikrishnan, ISP Program Director
Maria Johnson, GTA Program Director
Max Smart, Deputy ISP Program Director
Jim Cook, GTA Program Director
Kathy DuBose, Coordinator, JLAC

CORRECTIVE ACTION PLAN

Status Date	Report No.	Report Title		
9/24/2019	2019-186	STATE OF FLORIDA COMPLIANCE AND INTERNAL CONTROLS OVER FINANCIAL REPORTING AND FEDERAL AWARDS for Fiscal Year Ended June 30, 2018		
Contact Person	Program	Process	Phone No.	
Sally Huggins	EXEC	Office of Financial Management		
Activity	Accountability		Schedule	
	Responsible Unit	Coordinating Unit	Repeat Finding	Anticipated Completion Date
	Operational Accounting			January 18, 2019
Finding				
No.	AM 2018-01	The FDOR understated Receivables, net and Unavailable revenue due to an error in the preparation of year-end accrual entries.		
Date				
Recommendation	We recommend that the GTA program enhance the review process to promote the timely detection and correction of errors in the preparation of year-end accrual entries. Additionally, we recommend that the GTA program ensure that staff preparing and reviewing fiscal year-end reporting calculations and related accrual entries have sufficient training to perform the calculations and make appropriate accrual entries.			
Original Response	FDOR concurs with the recommendation and has implemented an additional level of management review and associated training to ensure proper preparation of year-end accrual entries.			
Status Updates	OIG 9/24/2019 While OFM has provided information about steps taken to correct this finding, we are not verifying it as complete until after the results of the AG's annual financial audit.			
<input type="checkbox"/> Open <input type="checkbox"/> Management assumes risk <input type="checkbox"/> Partially complete <input checked="" type="checkbox"/> Complete pending OIG verification <input type="checkbox"/> Complete				

CORRECTIVE ACTION PLAN

Status Date	Report No.	Report Title		
6/30/2019	AG 2019-124	SUNTAX Information Technology Operational Audit		
Contact Person	Program	Process	Phone No.	
Robert Clark	ISP	SUNTAX Security	850-717-6976	
Activity	Accountability		Schedule	
Limit Access Privileges	Responsible Unit	Coordinating Unit	Repeat Finding	Anticipated Completion Date
	ISP	Information Security Management	Yes	8/31/2019
Finding	Some Department users had inappropriate and unnecessary SUNTAX access privileges. Similar findings were noted in prior audits of the Department.			
No.	1			
Date	2/14/2019			
Recommendation	We again recommend that Department management limit user access privileges to SUNTAX to promote an appropriate separation of duties and restrict users to only those access privileges necessary for the users' assigned job duties. We also recommend that Department management ensure that user accounts are individually assigned to promote accountability for actions taken.			
Original Response	We agree with the finding and recommendations. We will identify user accounts that have inappropriate levels of access to SUNTAX databases and server operating systems and restrict them. We will ensure that duties with update access are separated between SUNTAX development and production environments, and between users with access to update taxpayers addresses and billing documents. SUNTAX accounts will be reviewed to ensure there is no sharing among multiple users. The roles will have their descriptions and access privileges documented to assist the process to review appropriateness.			
Status Updates	<p>Action Item 1: Identify users with inappropriate access.</p> <p>6/30/19: This information was provided by the AG's office to ISP. We consider this task closed.</p> <p>Action Item 2: Remove unnecessary or inappropriate access.</p> <p>6/30/19: ISP used the data from the AG's office to identify users with inappropriate or unnecessary access. ISP and GTA are reviewing each user individually and will make sure that the user's access level is appropriate and necessary. This task is expected to be completed by 7/31/19.</p> <p>Action Item 3: ISP and GTA will work together to ensure roles allow for separation of duties.</p> <p>6/30/19: New roles have been or are in the process of being created for developers and users that allow for separation of duties. The new roles completed are currently being tested. This task is expected to be completed by 8/31/19.</p> <p>Action Item 4: Ensure that accounts are not shared between users.</p> <p>6/30/19: ISP has identified the shared accounts mentioned in the finding. These accounts are admin accounts for the various SUNTAX system components. Due to limitations within SAP, it is not possible to create an admin account for each member of the admin team. Access to these three accounts is restricted to use by only one team within ISP. When these accounts are used, the admin's IP address is captured in system logs. Account usage can be tied back to a single user for accountability purposes. ISP is working on a process to review and monitor these logs.</p> <p>Action Item 5: SUNTAX role descriptions and access privileges will be documented.</p> <p>6/30/19: ISP has pulled all role data from the SUNTAX system. ISP and GTA will document descriptions and access privileges for each role. This task is expected to be completed by 8/30/19.</p>			
<input checked="" type="checkbox"/> Open <input type="checkbox"/> Management assumes risk <input type="checkbox"/> Partially complete <input type="checkbox"/> Complete pending OIG verification <input type="checkbox"/> Complete				

CORRECTIVE ACTION PLAN

Status Date	Report No.	Report Title		
6/30/2019	AG 2019-124	SUNTAX Information Technology Operational Audit		
Contact Person	Program	Process	Phone No.	
Robert Clark	ISP	SUNTAX Security	850-717-6976	
Activity	Accountability		Schedule	
Improvement of ISP's Account Deactivation Process	Responsible Unit	Coordinating Unit	Repeat Finding	Anticipated Completion Date
	ISP	Information Security Management	Yes	May 1, 2019
Finding	As similarly noted in prior audits, the Department did not timely deactivate the SUNTAX access privileges of some former employees.			
No.	2			
Date	2/14/2019			
Recommendation	We again recommend that Department management ensure that the SUNTAX user access privileges are timely deactivated upon a user's separation from Department employment.			
Original Response	We agree with the finding and recommendations. An extra verification step will be added to the account deactivation process to ensure user access is removed in a timely manner after every separation from the Department and when a user transfers internally to another position that does not require SUNTAX access.			
Status Updates	<p>Action Item 1: Add extra verification step to account deactivation process.</p> <p>6/30/19: ISP has added an additional internal control to provide weekly oversight of access removal tasks to ensure that ISP accurately and timely removes access from separated users. This process was started in April 2019. We consider this task closed.</p> <p>Action Item 2: ISP conducts quarterly reviews where lists of all active accounts are reconciled with employee separation/transfer reports. This process was started in April 2019. We consider this task closed.</p> <p>We consider this finding closed.</p>			
<input checked="" type="checkbox"/> Open <input type="checkbox"/> Management assumes risk <input type="checkbox"/> Partially complete <input type="checkbox"/> Complete pending OIG verification <input type="checkbox"/> Complete				

CORRECTIVE ACTION PLAN

Status Date	Report No. AG 2019-124	Report Title SUNTAX Information Technology Operational Audit		
Contact Person Robert Clark	Program ISP	Process SUNTAX Security	Phone No. 850-717-6976	
Activity	Accountability		Schedule	
Access Privileges Review	Responsible Unit	Coordinating Unit	Repeat Finding	Anticipated Completion Date
	ISP	Information Security Management	Yes	May 1, 2019
Finding	Department procedures for conducting periodic reviews of user access privileges continue to need improvement to ensure the appropriateness of SUNTAX user access privileges.			
No.	3			
Date	2/14/2019			
Recommendation	We again recommend that Department management perform comprehensive and effective periodic reviews of SUNTAX user access privileges to verify that the access privileges remain appropriate. Department management should reassess the frequency of the periodic reviews of SUNTAX user access privileges to better align with the criticality of the system and the confidential and sensitive data therein.			
Original Response	We agree with the finding and recommendation. We currently conduct annual reviews of SUNTAX user access privileges. We will need to assess this process and ensure that it meets our needs and is aligned with the criticality of the system.			
Status Updates	6/30/2019 – This task has been completed by GTA. GTA has increased their review cycle from annually to semiannual. The reviews will now include all SUNTAX users, not just those within GTA. We consider this finding closed.			
<input checked="" type="checkbox"/> Open <input type="checkbox"/> Management assumes risk <input type="checkbox"/> Partially complete <input type="checkbox"/> Complete pending OIG verification <input type="checkbox"/> Complete				

CORRECTIVE ACTION PLAN

Status Date	Report No.	Report Title		
6/30/2019	AG 2019-124	SUNTAX Information Technology Operational Audit		
Contact Person	Program	Process	Phone No.	
Robert Clark	ISP	SUNTAX Security	717-6976	
Activity	Accountability		Schedule	
	Responsible Unit	Coordinating Unit	Repeat Finding	Anticipated Completion Date
			Yes	11/30/2019
Finding	Certain security controls related to logical access, user authentication, and logging and monitoring continue to need improvement to ensure the confidentiality, integrity, and availability of SUNTAX data and Department IT resources.			
No.	4			
Date	2/14/2019			
Recommendation	We recommend that Department management improve certain security controls related to logical access, user authentication, and logging and monitoring for SUNTAX and related IT resources to ensure the continued confidentiality, integrity, and availability of SUNTAX data and related IT resources.			
Original Response	We agree with the finding and recommendations. ISP will work with the General Tax Administration business process to implement improvements and increase security controls.			
Status Updates	<p>ISP is taking the following steps to address this finding:</p> <ul style="list-style-type: none"> • Work with GTA to ensure all necessary steps are taken to ensure employees have access privileges only to those transactions associated with their job descriptions. • Explore options for improving logging and monitoring of system activities. <p>Appropriate changes to improve user authentication controls have been made. We consider this task closed.</p> <p>Additional information is available in conjunction with the Auditor General's confidential report related to AG Report No. 2019-124.</p>			
<input type="checkbox"/> Open <input type="checkbox"/> Management assumes risk <input checked="" type="checkbox"/> Partially complete <input type="checkbox"/> Complete pending OIG verification <input type="checkbox"/> Complete				