CHIEF FINANCIAL OFFICER
JIMMY PATRONIS
STATE OF FLORIDA

July 6, 2017

The Honorable Jimmy Patronis
Chief Financial Officer
The Capitol, PL-11
Tallahassee, Florida 32399-0301

Dear CFO Patronis:

As required by Section 20.055, Florida Statutes, I am providing the Department's six-month status report of corrective actions taken in response to Auditor General Report Number 2017-089, *Department of Financial Services Florida Accounting Information Resource Subsystem (FLAIR),* published January 6, 2017.

If you have any questions, please do not hesitate to contact me.

Sincerely,

Leah Gardner for
Teresa Michael
Inspector General

TM/rlg
Enclosure
c: Robert Kneip, Chief of Staff
Kathy DuBose, Coordinator, Joint Legislative Auditing Committee
Charles Ghini, Chief Information Officer
Christina Smith, Director of Accounting & Auditing

FLORIDA DEPARTMENT OF FINANCIAL SERVICES
Teresa Michael • Inspector General
200 East Gaines Street • Tallahassee, Florida 32399-0312 • Tel. 850-413-3112 • Fax 850-413-4973
Email • Teresa.Michael@MyFloridaCFO.com

DEPARTMENT OF FINANCIAL SERVICES
OFFICE OF INSPECTOR GENERAL

SIX-MONTH FOLLOW-UP REPORT
STATUS OF CORRECTIVE ACTION

Reviewing Entity	Report No.	Report Title	Date Published
Auditor General	2017-089	Department of Financial Services Florida Accounting Information Resource Subsystem (FLAIR)	January 6, 2017

Finding 1	The access privileges for some FLAIR and network users did not promote an appropriate separation of duties and did not restrict users to only those functions necessary for assigned job duties.
Recommendation	Department management should improve controls to ensure that user accounts are uniquely assigned, timely deactivated when no longer needed or an employee terminates or transfers, and promote an appropriate separation of duties.
Responsible Divisions	Division Accounting and Auditing; Office of Information Technology
Original Response	We concur. The Division of Accounting and Auditing (A&A) will improve controls to ensure that user accounts are uniquely assigned and timely deactivated. The Office of Information Technology (OIT) terminated the shared desktop administrative account on September 26, 2016. Additionally, OIT implemented documented procedures for the payroll component program change management review process on December 1, 2016.
Six-month Follow-up:	July 6, 2017
Reported Status	The A&A has consolidated administrative functions and is currently updating access control procedures and the related desk procedures to ensure access is timely deactivated and accounts are uniquely assigned. The OIT terminated the shared desktop administrative account on September 26, 2016. Additionally, OIT implemented documented procedures for the payroll component change management review process on December 1, 2016.
Expected Completion Date for Corrective Action	A&A: October 1, 2017 OIT: December 1, 2016
OIG Assessment	**Partially Closed**. Based on the information provided, it appears that A&A and OIT management initiated action to address most of the recommendation. The OIG will continue monitoring OIT efforts to ensure the procedures implemented for the payroll component change management are working as intended. Specifically, programmers' changes are reviewed by another staff member to ensure there is an appropriate segregation of duties and there is documentation that supports a supervisor's review of the Analyst Checklist. Also, we will review A&A's supporting documentation when provided.

DEPARTMENT OF FINANCIAL SERVICES
OFFICE OF INSPECTOR GENERAL

SIX-MONTH FOLLOW-UP REPORT
STATUS OF CORRECTIVE ACTION

Reviewing Entity	Report No.	Report Title	Date Published
Auditor General	2017-089	Department of Financial Services Florida Accounting Information Resource Subsystem (FLAIR)	January 6, 2017

Finding 2	The Department's procedures and processes for conducting periodic reviews of user access privileges need improvement to ensure access privileges assigned to users remain appropriate.
Recommendation	Department management should ensure that access control procedures are up to date, all periodic reviews are performed as required and include all assigned user access privileges, and documentation of completed reviews is maintained.
Responsible Divisions	Division of Accounting and Auditing; Office of Information Technology
Original Response	We concur. The Division of Accounting and Auditing will update DACA for OLO 4390 Access Control Business Process Procedure used for authorizing and reviewing DAC user access privileges. On October 6, 2016, OIT implemented a process for quarterly reviews of privileged administrator accounts and the first quarterly review was completed on October 28, 2016. Additionally, on October 11, 2016, OIT modified the COBOL access review process to include tracking of review responses. The OIT also submitted a change request on November 29, 2016, to incorporate an additional report into the DAC access review process which includes the additional access levels.
Six-month Follow-up:	July 6, 2017
Reported Status	The A&A is currently completing an OLO 4390 access control procedure review and update. On November 29, 2016, OIT submitted a change request to incorporate an additional report into the DAC access review process which includes the additional access levels. The reporting change will be completed in June 2017. Additionally, OIT completed the first quarterly review of privileged administrator accounts on October 28, 2016. The COBOL access review process was also updated on October 11, 2016, to include tracking of review responses.
Expected Completion Date for Corrective Action	A&A: October 1, 2017 OIT: June 2017
OIG Assessment	**Partially Closed**. Based on the information provided, it appears that A&A and OIT management initiated action to address most of the recommendation. The OIG will continue monitoring OIT efforts until documentation is provided that demonstrates OIT implemented corrective actions related to the the periodic review of access privileges for the DAC State Chief Financial Officer Files (SC) function and the related DAC SC Electronic Funds Transfer (EFT) Authorization Inquiry Request (ET) mini-menu function. The OIG will review A&A's supporting documentation when provided.

DEPARTMENT OF FINANCIAL SERVICES
OFFICE OF INSPECTOR GENERAL

SIX-MONTH FOLLOW-UP REPORT
STATUS OF CORRECTIVE ACTION

***** Confidential Finding *****

Reviewing Entity	Report No.	Report Title	Date Published
Auditor General	2017-089	Department of Financial Services Florida Accounting Information Resource Subsystem (FLAIR)	January 6, 2017
Finding 3	Certain security controls related to physical security, user authentication, and configuration management need improvement to ensure the confidentiality, integrity, and availability of Department data and IT resources.		
Recommendation	Department management should improve certain security controls related to physical security, user authentication, and configuration management to ensure the confidentiality, integrity, and availability of Department data and IT resources.		
Responsible Division	Office of Information Technology		
Original Response	As of October 19, 2016, OIT concluded implementation of corrective action to address physical security related concerns. The OIT will evaluate the additional security concerns and, where appropriate, implement additional controls.		
Six-month Follow-up:	July 6, 2017		
Reported Status	The OIT implemented modifications to the authentication controls in April 2017. Additionally, procedures related to configuration management and physical security were enhanced. The OIT will continue to evaluate security controls and make enhancements, where appropriate.		
Expected Completion Date for Corrective Action	No date provided.		
OIG Assessment	**Partially Closed.** Based on the information provided, it appears that OIT management initiated some action to address the recommendation. The OIG will continue to monitor this finding until DIS fully implements corrective action or documents the acceptance of risk for the findings related to physical security, user authentication, risk acceptance process and configuration management.		

Note: Due to the confidential nature of this finding, and to ensure the security of DFS systems, detailed information is not provided in this status report.