

**DEPARTMENT OF FINANCIAL SERVICES  
OFFICE OF INSPECTOR GENERAL**

**SIX-MONTH FOLLOW-UP REPORT  
STATUS OF CORRECTIVE ACTION**

<b>Reviewing Entity</b>	<b>Report</b>	<b>Report Title</b>	<b>Date Published</b>
State of Florida Auditor General	AG 2020-095	Florida Accounting Information Resource Subsystem (FLAIR)	1/13/2020
<b>Finding 1</b>	The Department did not always timely deactivate the FLAIR user accounts with access privileges to the Central Accounting Component and Payroll Component when employees separated from Department employment. Similar findings were noted in our report No. 2019-068.		
<b>Recommendation</b>	We recommend that Department management ensure that FLAIR user accounts with CAC and Payroll Component access privileges are timely deactivated upon the employee's separation from Department employment.		
<b>Responsible Division</b>	Division of Accounting & Auditing		
<b>Original Response</b>	<p>The Department concurs. The Division of Accounting &amp; Auditing (A&amp;A) has revised desktop procedures and provided training to additional staff on the administrative team to assist in prevention of untimely access deactivation. A&amp;A will continue to monitor access control reports as well as work with Agency personnel to ensure timely deactivation of access. On December 13, 2019, A&amp;A met with Agency Admin Directors and discussed the importance of monitoring agency access and timely deactivation. A&amp;A will continue outreach to agencies in an effort to improve this process.</p> <p>Office of Information Technology (OIT) response: Although this is a manual process, due to our defense in depth strategy the risk is low, as the users must have an active "Active Directory" account to gain access to FLAIR. OIT's FLAIR team is researching potential methods of identifying potentially separated or role/duty changes by DFS users. If this type of report can be generated, this will minimize the risk of user privileges not being deactivated timely. Additional funding through an LBR would be necessary for automation to occur for this process.</p>		
<b>Six-month Follow-up:</b>	July 13, 2020		
<b>Reported Status</b>	A&A continues to monitor access, review procedures and outreach to agencies regarding timely deactivation. There are also three team members on the administrative team that are able to remove access. In addition, the Administrative team has created a team calendar to identify future dates of when individuals will no longer work with the Division to help ensure timely deactivation.		
<b>Expected Completion Date for Corrective Action</b>	Complete		
<b>OIG Assessment</b>	Based on A&A's response, it appears that corrective action was taken to address the finding.		

**DEPARTMENT OF FINANCIAL SERVICES  
OFFICE OF INSPECTOR GENERAL**

<b>Reviewing Entity</b>	<b>Report</b>	<b>Report Title</b>	<b>Date Published</b>
State of Florida Auditor General	AG 2020-095	Florida Accounting Information Resource Subsystem (FLAIR)	1/13/2020
<b>Finding 2</b>	As similarly noted in our report No. 2019-068, the Department had not established a comprehensive policy for the performance of background screenings of employees and contracted consultants in positions of special trust. Additionally, background screening processes for contracted consultants need improvement to ensure all consultants are screened prior to the start of the contracted work.		
<b>Recommendation</b>	We again recommend that Department management finalize the comprehensive Departmentwide background screening policy and related procedures and ensure the timely performance of background screenings of contracted consultants in positions of special trust.		
<b>Responsible Division</b>	Division of Administration Office of Information Technology		
<b>Original Response</b>	<p>The Department concurs. The Division of Administration (ADM) will continue its efforts to establish a comprehensive Departmentwide background screening policy and related procedures, both of which will be designed to ensure the timely performance of background screenings of employees and contracted consultants, being designated into positions of special trust.</p> <p>Office of Information Technology (OIT) response: This is a moderate risk. OIT is actively working to assure all OIT workers are screened timely prior to onboarding and rescreened as recommended in the DFS draft policy. OIT will make the necessary changes to follow the approved DFS policy once completed and approved in June 2020. OIT is also having the identified consultants during the 2019 Audit rescreened and to be completed no later than February 21, 2020.</p>		
<b>Six-month Follow-up:</b>	July 13, 2020		
<b>Reported Status</b>	<p>OIT - OIT has made revisions to the internal OIT Procedure and will be finalizing the revisions based on the new DFS background screening policy once it is finalized and published. OIT is actively working to rescreen any workers outside of the timeframe of 5 years as identified in the DFS draft policy. Consultants that were in questions during the FLAIR 2019 audit have been rescreened.</p> <p>ADM - The comprehensive Departmentwide background screening policy is still pending with senior leadership team.</p>		
<b>Expected Completion Date for Corrective Action</b>	December 2020		
<b>OIG Assessment</b>	<b>Partially closed.</b> Based on the information provided, it appears some corrective action to address this finding was initiated.		

**DEPARTMENT OF FINANCIAL SERVICES  
OFFICE OF INSPECTOR GENERAL**

<b>Reviewing Entity</b>	<b>Report</b>	<b>Report Title</b>	<b>Date Published</b>
State of Florida Auditor General	AG 2020-095	Florida Accounting Information Resource Subsystem (FLAIR)	1/13/2020
<b>Finding 3</b>	Certain security controls related to physical security, user authentication, and logging and monitoring continue to need improvement to help ensure the confidentiality, integrity, and availability of FLAIR data and other Department IT resources.		
<b>Recommendation</b>	We recommend that Department management improve certain security controls related to physical security, user authentication, and logging and monitoring to ensure the confidentiality, integrity, and availability of FLAIR data and other Department IT resources.		
<b>Responsible Division</b>	Office of Information Technology Division of Accounting and Auditing		
<b>Original Response</b>	<p>The Department concurs. The risk involved with this finding is low, as we have defense in depth; and we are continuing to improve overall processes and timeliness on our physical security and user authentication processes. ISO is defining the current operational guides for logging and monitoring controls and reports.</p> <p>The Division of Accounting and Auditing is currently working with the Department's Office of Information Technology to strengthen authentication controls.</p>		
<b>Six-month Follow-up:</b>	July 13, 2020		
<b>Reported Status</b>	Ongoing. ISO is continuing to define the current operational guides for logging and monitoring controls and reports. The reports will be built in accordance with those requirements.		
<b>Expected Completion Date for Corrective Action</b>	December 31, 2020		
<b>OIG Assessment</b>	<b>Partially closed.</b> Based on the information provided, it appears some corrective action to address this finding was initiated.		