apd
agency for persons with disabilities
State of Florida

Ron DeSantis
Governor

Barbara Palmer
Director

State Office

4030 Esplanade Way
Suite 380
Tallahassee
Florida
32399-0950

(850) 488-4257
Fax:
(850) 922-6456

Toll Free:
(866) APD-CARES
(866-273-2273)

February 25, 2020

Barbara Palmer, Director
Agency for Persons with Disabilities
4030 Esplanade Way, Suite 380
Tallahassee, FL 32399-0950

Re: OIG# 181129-01, Status of Corrective Actions, Auditor General Report No. 2020-018, Information Technology General Controls

Dear Director Palmer:

As required by section 20.055(6)(h), Florida Statutes, the corrective action status report for Auditor General Report Number 2020-018, Information Technology General Controls, is attached. The report details the implementation or current status of each recommendation.

Please contact me if you have any questions.

Sincerely,

Erin Romeiser

Erin Romeiser
Inspector General

Enclosure

cc: JLAC@leg.state.fl.us
Melinda M. Miguel, Chief Inspector General
Ms. Sherrill F. Norman, Auditor General
David Dobbs, Chief of Staff

Status of Corrective Actions for Auditor General Report No. 2020-018, Information Technology General Controls

Status Type	**Report No.**	**Report Title**
STATUS UPDATE - 6 MONTHS	2020-018	Information Technology General Controls
Contact Person	**Program/Process**	**Phone No.**
Michael Sodders	Information Technology	850-488-4870

Activity	**Accountability**	**Schedule**	
iBudget Florida Allocation Methodology and Algorithm	**Responsible Unit**	**Repeat Finding**	**Anticipated Completion Date**
	Information Technology	No	N/A

Finding: **No.** 1 **Date** August 27, 2019	**Information Security Program** The Agency's *Information Security Program Policy* did not encompass or reference significant aspects of a comprehensive information security program.
Recommendation	**We recommend that Agency management ensure that the Agency information security program includes all relevant security policies and procedures to appropriately protect the information and information systems that support the operations and assets of the Agency.**
Original Response/ Action Plan	The Agency concurs with this finding. The Agency will write the recommended security awareness training policy/procedure. The Agency will formally add its current incident handling protocol, which includes requirements for categorizing security incidents, to its *Information Security Incident and Breach Response Policy*. The Agency will write the recommended Agency-managed server data backup policy/procedure. The Agency will write the recommended firmware patches policy/procedure.
Status Updates □**Open** □**Partially complete** □**Complete** ☒**Complete pending verification by the Auditor General** □**Management assumes risk**	The agency is in the process of drafting all-new information security policies and procedures, built upon the frameworks of the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity and the Florida Cybersecurity Standards (60GG-2 F.A.C.), which will supersede existing policies and procedures. These new policies and procedures include the above-mentioned components of Information Security Awareness Training, Incident and Breach Response, Data Backup, and Software/Firmware Patching.

Finding:		**Security Awareness Training** Security awareness training for Agency employees was not always completed timely.
No.	**2**	
Date	August 27, 2019	
Recommendation		**We recommend that Agency management ensure security awareness training is timely completed in accordance with AST rules.**
Original Response/ Action Plan		The Agency concurs with this finding. The Agency is analyzing the causes of this problem and will develop strategies to address it.
Status Updates **□Open** **□Partially complete** **□Complete** **☒Complete pending verification by the Auditor General** **□Management assumes risk**		The agency is working toward this goal. Efforts made to date include direct communications from Chief of Staff to agency employees on the importance of completing information security training, and Human Resources improvements in employee training completion tracking. Further scrutiny of the issue, along with development of new strategies, will continue in an on-going fashion.

Finding:		**Computer Security Incident Response** Agency computer security incident response processes need improvement.
No.	**3**	
Date	August 27, 2019	
Recommendation		**We recommend that Agency management ensure that cybersecurity incidents are sufficiently assessed and documented, CSIRT meetings are conducted at least quarterly, and CSIRT members receive annual training as required by AST rules.**
Original Response/ Action Plan		The Agency concurs with this finding. The Agency will exercise more care to ensure Incident documentatión is complete. The Agency will ensure all regularly scheduled Quarterly CSIRT meetings occur. The Agency will deliver training to the CSIRT more formally.

Status Updates ☐**Open** ☐**Partially complete** ☐**Complete** ☒**Complete pending verification by the Auditor General** ☐**Management assumes risk**	The agency has been ensuring the completeness of incident documentation, that all regularly scheduled quarterly CSIRT meetings occur, and more formal delivery of training to CSIRT.

Finding:		**Timely Disabled Network Access Privileges** The Agency did not timely disable the network access privileges for some former employees.
No.	**4**	
Date	August 27, 2019	
Recommendation		**To minimize the risk of compromise to Agency data and IT resources, we recommend that Agency management ensure that network access privileges are timely disabled upon an employee's separation from Agency employment. In addition, the Agency should retain records evidencing the dates accounts are disabled.**
Original Response/ Action Plan		The Agency concurs with this finding. The Agency is already taking steps to address this finding by ensuring closer coordination between Information Security and Human Resources, and will continue in these efforts.
Status Updates ☐**Open** ☐**Partially complete** ☐**Complete** ☒**Complete pending verification by the Auditor General** ☐**Management assumes risk**		The agency is continuing to improve coordination between Human Resources and Information Security to address this issue. To date, efforts include regular reports from Human Resources on terminated employees, and a dedicated communications channel between Information Security and Human Resources to facilitate communication on employee access control matters.

Status of Corrective Actions for Auditor General Report No. 2020-018, Information Technology General Controls

Finding:		**Periodic Access Review** Agency policies and procedures for periodic reviews of access privileges need improvement.
No.	5	
Date	August 27, 2019	
Recommendation		**We recommend that Agency management develop documented procedures to facilitate effective periodic reviews of all user accounts, including all privileged administrative accounts.**
Original Response/ Action Plan		The Agency concurs with this finding. The agency is developing procedures to address this finding.
Status Updates □**Open** □**Partially complete** □**Complete** ☒**Complete pending verification by the Auditor General** □**Management assumes risk**		The agency is in the process of drafting all-new information security policies and procedures, built upon the frameworks of the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity and the Florida Cybersecurity Standards (60GG-2 F.A.C.), which will supersede existing policies and procedures. These new policies and procedures include the above-mentioned component of Periodic Access Review.

Finding:		**Security Controls - Logical Access, User Authentication, Configuration Management, Logging and Monitoring, and Vulnerability Management** Certain security controls related to logical access, user authentication, configuration management, logging and monitoring, and vulnerability management need improvement.
No.	6	
Date	August 27, 2019	
Recommendation		**We recommend that Agency management improve certain security controls related to logical access, user authentication, configuration management, logging and monitoring, and vulnerability management to ensure the confidentiality, integrity, and availability of Agency data and other IT resources.**
Original Response/ Action Plan		The Agency concurs with this finding. The Agency will take actions to improve certain security controls.

Status of Corrective Actions for Auditor General Report No. 2020-018, Information Technology General Controls

Status Updates **□Open** **□Partially complete** **□Complete** **☒Complete pending verification by the Auditor General** **□Management assumes risk**	The agency has made progress on improving certain security controls and continues in the effort to complete the improvements.