Office of Inspector General
(850) 245-1360

Building C, Suite 3C
2601 South Blair Stone Road
Tallahassee, Florida 32399

Florida Department of Agriculture and Consumer Services
Commissioner Nicole "Nikki" Fried

DATE: December 13, 2021

TO: Nicole Fried, Commissioner

FROM: Angela H. Roddenberry, Inspector General

SUBJECT: 6-Month Status Report for Auditor General (AG) Report No. 2021-218: Department of Agriculture and Consumer Services - Information Technology General Controls

In accordance with Section 20.055(6)(h), Florida Statutes, the Office of Inspector General is submitting the 6-Month Status of Corrective Actions Taken for AG Report No. 2021-218: Department of Agriculture and Consumer Services - Information Technology General Controls. This report details the status of each audit recommendation as reported to us by appropriate management.

If you have any questions, please contact me at (850) 245-1360 or Angela.Roddenberry@fdacs.gov.

Enclosure

cc: Matthew Van Name, Assistant Commissioner/Chief of Staff
Eric Brown, Chief Information Officer
Benita Byard-Williams, Information Security Manager
Joint Legislative Auditing Committee

Six-Month Status of Corrective Actions Taken
Auditor General Report No. 2021-218, Department of Agriculture and Consumer Services – Information Technology General Controls

Finding 1:	**IT Asset Management** The Department did not maintain an up-to-date network diagram that included all high-risk network devices or a complete and accurate server inventory list to facilitate the monitoring, testing, and evaluation of IT resources to ensure the confidentiality, integrity, and availability of Department data and IT resources.
Recommendation:	We recommend that Department management maintain an up-to-date network diagram that includes all high-risk network devices and a complete and accurate inventory of servers to facilitate the monitoring, testing, and evaluation of IT resources.
Report Response:	We concur. The department's network diagrams have been updated. In addition, a server inventory has been developed to provide an accurate listing of servers to assist information technology management in ensuring the confidentiality, integrity, and availability of Department data and IT resources.
6-Month Status:	According to management, corrective action is complete.
Finding 2:	**Information Security Manager** Contrary to State law, the Department's Information Security Manager (ISM) did not report directly to the Commissioner of Agriculture for information security duty purposes.
Recommendation:	We recommend that Department management take steps to ensure that, for information security duty purposes, the Department ISM reports directly to the Commissioner in accordance with State law.
Report Response:	We concur. The department has updated the position description of the ISM to report to the Commissioner of Agriculture for all information security duty purposes as outlined in Section 282.318, Florida Statutes.
6-Month Status:	According to management, corrective action is complete.
Finding 3:	**Computer Security Incident Response** The Department Computer Security Incident Response Team did not convene at least quarterly to review, at a minimum, established processes and escalation protocols. In addition, Team members did not receive annual training to promote prompt and appropriate responses to cybersecurity events.

Recommendation:	We recommend that Department management update CSIRT policies and procedures to align to DMS rules and ensure that CSIRT quarterly meetings and annual training occur as specified in DMS rules.
Report Response:	We concur. The department is conducting quarterly CSIRT meetings and has scheduled meetings for the remainder of the year. Members of the CSIRT have completed online training to promote prompt and appropriate responses to cybersecurity events. Department administrative policy and procedures have been updated to include the annual training requirement.
6-Month Status:	According to management, corrective action is complete.
Finding 4:	**Disaster Recovery Planning** Department and Division of Licensing (Division) disaster recovery plans, annual testing, and related policies and procedures need improvement to ensure that critical Department and Division operations may be timely resumed in the event of a disaster or other interruption in service.
Recommendation:	We recommend that Department management update DR policies and procedures to require annual testing of Department and Division DR plans and that Department and Division management ensure that comprehensive live exercises of all DR plans are conducted annually, the results of the testing are documented, and necessary modifications identified during testing are incorporated into the applicable DR plan.
Report Response:	We concur. The department is continuing to improve its disaster recovery capabilities by increasing resources at our disaster recovery facility. The department is creating a unified disaster recovery plan and revising disaster recovery policies to ensure that all critical operations resume in a timely manner in the event of a disaster or other interruption in service.
6-Month Status:	According to management, department management has updated disaster recovery policies and procedures to require annual testing and annual exercising of the department's disaster recovery plans. These documents will be modified based on test and exercise results. The department continues to improve its disaster recovery capabilities to ensure all critical operations resume in a timely manner in the event of a disaster or other interruption in service.
Finding 5:	**Backup Controls** Department and Division controls need improvement to ensure that backups for Department and Division servers are appropriately performed and periodically tested for recoverability and that Department off-site storage locations for backup media are geographically separated from the primary operating locations.

Recommendation:	We recommend that Department management enhance policies and procedures to include periodic recoverability testing of backups and Department and Division management ensure that all servers are timely backed up, backups are periodically tested for recoverability, and backup media is stored at locations geographically separated from primary operating locations.
Report Response:	We concur. The department has implemented procedures to ensure that backups are performed and periodically tested for recoverability. All backups are now consolidated into the department's enterprise data backup solution which is stored at a geographically separate location from the department's primary data center.
6-Month Status:	According to management, the department has followed enhanced procedures and documented successful, periodic tests of recoverability. The department continues to improve its backup controls to ensure that all backup data is consolidated in the department's enterprise data backup solution at a geographically separate location.
Finding 6:	**Security Controls** Certain security controls related to logical access, physical access, tape encryption, vulnerability management, configuration management, user authentication, and logging and monitoring need improvement to ensure the confidentiality, integrity, and availability of Department data and IT resources.
Recommendation:	We recommend that Department management improve certain security controls related to logical access, physical access, tape encryption, vulnerability management, configuration management, user authentication, and logging and monitoring to ensure the confidentiality, integrity, and availability of Department data and IT resources.
Report Response:	We concur. The department continues to address and improve security controls by incorporating new policies, procedures, and processes. In addition, the department has enhanced and strengthened our security controls by implementing new hardware and software solutions.
6-Month Status:	According to management, corrective action is complete.