STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2021-218
June 2021

DEPARTMENT OF AGRICULTURE AND CONSUMER SERVICES

Information Technology General Controls

Sherrill F. Norman, CPA
Auditor General

Commissioner of Agriculture

The Department of Agriculture and Consumer Services is established by Section 20.14, Florida Statutes. The head of the Department is the Commissioner of Agriculture. The Honorable Nicole Fried served as Commissioner during the period of our audit.

The team leader was Arthur Wahl, CPA, CISA, and the audit was supervised by Hilda S. Morgan, CPA, CISA.

Please address inquiries regarding this report to Brenda Shiner, CISA, Audit Manager, by e-mail at brendashiner@aud.state.fl.us or by telephone at (850) 412-2946.

This report and other reports prepared by the Auditor General are available at:

FLAuditor.gov

Printed copies of our reports may be requested by contacting us at:

State of Florida Auditor General

Claude Pepper Building, Suite G74 · 111 West Madison Street · Tallahassee, FL 32399-1450 · (850) 412-2722

DEPARTMENT OF AGRICULTURE AND CONSUMER SERVICES

Information Technology General Controls

SUMMARY

This operational audit of the Department of Agriculture and Consumer Services (Department) focused on evaluating selected information technology (IT) general controls. Our audit disclosed the following:

Finding 1: 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.

Finding 2: Contrary to State law, the Department's Information Security Manager did not report directly to the Commissioner of Agriculture for information security duty purposes.

Finding 3: 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.

Finding 4: 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.

Finding 5: 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.

Finding 6: 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.

BACKGROUND

The Department of Agriculture and Consumer Services (Department) was created and organized in accordance with State law[1] to support and promote the State's agriculture, protect the environment, safeguard consumers, and ensure the safety and wholesomeness of food. The Department operates through 12 divisions and 10 offices, including the Office of Agriculture Technology Services (OATS) and the Division of Licensing (Division). The primary functions of OATS are to administer the Department's information technology (IT) operations and provide IT services such as network operations, e-mail, collaboration tools, business application support, Web-based information systems, data administration,

[1] Section 20.14, Florida Statutes.

enterprise storage, help desk, office automation, and project management. The Division administers the State's concealed weapon licensing program and oversees the private investigative, private security, and recovery services industries. The Division is also responsible for managing Division servers.

FINDINGS AND RECOMMENDATIONS

Finding 1: IT Asset Management

Effective IT asset management controls include the maintenance of a complete, accurate, and up-to-date inventory of IT resources (e.g., physical and virtual servers, network devices, and databases) to ensure that management is knowledgeable of all IT resources for which they are responsible for managing. Further, a complete, accurate, and up-to-date inventory is necessary for the effective monitoring, testing, and evaluation of IT resources and the timely implementation of the latest relevant security patches and other critical updates (e.g., service packs and hot fixes) from IT vendors. Department of Management Services (DMS) rules[2] require each State agency to ensure that physical devices and systems within the organization are inventoried and managed. Department of Agriculture and Consumer Services (Department) policies and procedures[3] also required a current network diagram be maintained.

To evaluate the effectiveness of Department IT asset controls for managing Department high-risk network devices and servers, we requested from Department personnel the network diagram and inventory of Department servers. In response to our request, Department personnel provided the network diagram as of December 20, 2019, and a server inventory list as of January 17, 2020, that included 530 Department servers. However, our audit found that neither the network diagram nor the server inventory list was complete or accurate. Specifically, we found that the network diagram did not reflect 86 of the 95 high-risk network devices and Department management provided two additional server inventory lists that included 54 other servers. According to Department management, the high-risk network devices were omitted from the network diagram due to an oversight and that, because an official server inventory list was not maintained, a complete and accurate list of servers did not exist. Department management indicated that, subsequent to our audit inquiry, the network diagram was updated to include the omitted high-risk network devices.

Maintenance of an up-to-date network diagram that includes all high-risk network devices and a complete and accurate inventory of servers facilitates 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.

[2] DMS Rule 60GG-2.002(1)(a), Florida Administrative Code.

[3] Department Administrative Policies and Procedures No. 8-17, *Systems and Communications Protection*.

Finding 2: Information Security Manager

State law[4] requires each State agency head to designate an information security manager (ISM) to administer the agency's IT security program. State law specifies that, for information security duty purposes, the ISM is to report directly to the agency head. Organizational placement of the ISM outside the line of authority of those responsible for daily Department IT operations would maximize the independence and objectivity of the ISM function.

Our examination of Department records disclosed that, in January 2020, the Commissioner of Agriculture (Commissioner) designated an ISM to administer the Department IT security program who was to report directly to the Chief Technology Officer within OATS, rather than the Commissioner. According to Department management, while the Commissioner was knowledgeable of the statutory requirement for the ISM to report directly to the Commissioner for information security duty purposes, the ISM reported directly to the Chief Technology Officer due to operational job responsibilities outside information security. Notwithstanding, the ISM directly reporting to the Chief Technology Officer reduces Department management's assurance related to the objectivity and independence of the ISM function and does not comply with State law.

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.

Finding 3: Computer Security Incident Response

DMS rules[5] require State agencies to establish and maintain response processes and procedures and validate execution capability to ensure timely agency response for detected cybersecurity incidents. State agencies are also required to establish a Computer Security Incident Response Team (CSIRT) to respond to cybersecurity incidents. The CSIRT is to convene at least quarterly to review, at a minimum, established processes and escalation protocols, and CSIRT members are to receive incident response training annually.

As part of our audit, we conducted inquiries of Department management and staff and examined Department policies and procedures[6] and computer security incident response records. Our audit procedures found that, contrary to DMS rules, the policies and procedures did not require annual computer security incident response training for CSIRT members and, as of July 2020, the most recent training was conducted for one CSIRT member in March 2018. Additionally, while Department policies and procedures required quarterly CSIRT meetings to review established processes and escalation protocols, the last CSIRT meeting was in 2017 to discuss a specific Department computer security incident. In response to our audit inquiry, Department management indicated that the lack of annual training and quarterly CSIRT meetings was an oversight by the Department.

[4] Section 282.318(4)(a), Florida Statutes.

[5] DMS Rule 60GG-2.005(1)(a), Florida Administrative Code.

[6] Department Administrative Policies and Procedures No. 8-11, *Computer Security Incident Response Team*.

Absent compliance with DMS rules requiring CSIRT members to convene at least quarterly to review, at a minimum, established processes and escalation protocols, and receipt of annual training, the risk is increased that cybersecurity incidents will not be timely detected, appropriately responded to, and corrected.

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.

Finding 4: Disaster Recovery Planning

Disaster recovery (DR) planning is intended to facilitate the timely recovery of critical applications, data, and services in the event of a disaster or other interruption in service. DMS rules[7] require State agencies to develop and implement a DR plan, test the DR plan at least annually, and document the results of the test, including DR plan procedures that were successful and any modifications required to improve the DR plan. Furthermore, DMS rules[8] require State agencies to improve the DR plan and processes by incorporating lessons learned into future activities, including DR plans.

As part of our audit, we interviewed Department and Division of Licensing (Division) management and staff and examined Department DR policies and procedures[9] and Department and Division DR plans and testing records and found that, as of August 2020, both Department and Division DR controls need improvement. Specifically, we found that:

- Department DR policies and procedures only required DR plan testing every 3 years, contrary to DMS rules.
- The Department DR plan had not been updated since May 2010 and included inaccurate information such as the responsible personnel, network diagram, and server backups required for recovery.
- The most recent testing of the Department DR plan was a DR exercise of the Florida Fire Management Information System conducted in November 2015 and a tabletop exercise for Office 365 in 2019; however, neither exercise represented a complete test of the DR plan.
- While a separate DR plan was maintained for the Division and, according to Division management, DR plan testing was conducted in 2012 upon implementation of the contract with the off-site DR provider, evidence of the DR exercises was not retained and the DR plan had not been tested since 2012.

In response to our audit inquiry, Department management indicated that annual comprehensive testing of the DR plan was not done and the DR plan was not updated as necessary due to Department oversight. Additionally, Division management indicated that, since OATS was the owner of the off-site DR contract, the Division was unable to independently initiate DR exercises; however, the Division was working with OATS to coordinate future testing of the Division DR plan.

[7] DMS Rule 60GG-2.006(1), Florida Administrative Code.

[8] DMS Rule 60GG-2.006(2), Florida Administrative Code.

[9] Department Administrative Policies and Procedures No. 8-9, *Mission Critical Application Risk Assessment and Contingency Planning*.

DR policies and procedures designed in accordance with DMS rules and updated DR plans help ensure that Department and Division data will be readily recoverable and available when needed. Conducting comprehensive live exercises of DR plans annually, documenting DR test results, and incorporating necessary DR plan modifications identified during testing decreases the risk that critical Department and Division applications will not be timely and orderly resumed in the event of a disaster or other interruption of 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.

Finding 5: Backup Controls

Effective backup controls include policies and procedures for routinely duplicating or backing up data files and computer programs, ensuring off-site backup media storage locations are geographically separated from the primary operating locations, and establishing a recovery and restoration capability, including periodically testing backup media so that data and computer programs can be recovered and restored after a disruption or failure. DMS rules[10] require State agencies to ensure that backups of information are conducted, maintained, and tested.

OATS staff were responsible for performing server backups for Department-managed servers and Division-managed virtual servers. Division staff were responsible for performing server backups for Division-managed physical servers. As part of our audit, we interviewed Department and Division management and staff, reviewed Department backup policies and procedures,[11] and evaluated Department and Division backup processes, including the performance of daily and weekly backups and periodic recoverability testing of backups performed by Department and Division staff. Our audit procedures found that Department policies and procedures did not require periodic recoverability testing of the backups performed and, according to Department management as of January 17, 2020, recoverability tests of the backups performed by OATS staff were not conducted at a specified frequency. While Division management acknowledged that scheduled recoverability tests were not performed, Division management indicated that data restore processes were performed monthly to refresh data and troubleshoot data issues. However, our examination of Division records found that, as of February 2020, the last restore was performed in July 2019. In response to our audit inquiry, Department management indicated that the absence of procedures for and the conduct of recoverability tests was an oversight by management.

As noted in Finding 1, the Department did not maintain an official server inventory list, therefore limiting management's assurance regarding the accuracy and completeness of the information necessary to maintain accountability for all Department servers. Notwithstanding this limitation, from the list of servers provided by the Department, we evaluated the existence of backups as of January 30, 2020, for 44 of

[10] DMS Rule 60GG-2.003(5)(d), Florida Administrative Code.

[11] Department Administrative Policies and Procedures No. 8-2, *Department Information Technology Workers, Contractors, Providers, and Partners*.

the 307 production servers backed up by OATS and the 9 physical production servers backed up by the Division. Our evaluation of backup records found that:

- 3 of the production servers backed up by OATS were not appropriately backed up. Specifically, 1 server had not been backed up since the server was placed into production on August 1, 2019, another server had not been backed up since October 9, 2019, and a third server was not backed up during the period July 2019 through January 2020. According to Department management, the first server was not added to the backup process when placed into production, the second server was accidentally removed from the backup process while troubleshooting an application issue, and the third server was not backed up due to the age of the server and its incompatibility with the backup products used by the Department.
- A Division physical production server was not included in the Division backup schedule and therefore had never been backed up and 2 other Division physical production servers had not been backed up since August 2018. In response to our audit inquiry, Division management indicated that the 3 servers were not database servers or file stores and that the only data that changed were system and application logs, which they erroneously believed were not required to be backed up. Department management subsequently indicated that the servers were added to the backup schedule.

As part of our audit, we also evaluated Department off-site storage controls for backup media and found that the off-site storage controls need improvement. Specifically, we found that:

- The off-site storage location for backup tape media for the production servers backed up by the Division and two production servers backed up by OATS was another Department facility located within the same city as the Department data center in Tallahassee and, therefore, the backup tape media was stored in a location that was not geographically separated from the data center. According to Division management, they relied on OATS staff to provide the off-site storage location but were working with OATS staff to replicate the Division server data to the disaster recovery site located outside of Tallahassee. Department management indicated that the two servers backed up by OATS were subsequently decommissioned.
- Backup tapes and disks for Division of Food Safety (Food Safety) servers located at a Department facility in Tallahassee were stored off-site at the Department data center also located in Tallahassee and thus, also not geographically separated from the facility where the servers were located. In response to our audit inquiry, Department management indicated that OATS and Food Safety staff would work to find an acceptable off-site storage location geographically separated from the Tallahassee facility.

The absence of policies and procedures requiring periodic recoverability testing; the absence of timely, complete, and successful server backups for all servers; and the geographical proximity of the off-site backup media storage locations to the primary operating locations increase the risk that data on Department and Division server backups will not be readily recoverable and available when needed in response to unexpected events.

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.

Finding 6: Security Controls – Logical Access, Physical Access, Tape Encryption, Vulnerability Management, Configuration Management, User Authentication, and Logging and Monitoring

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit procedures disclosed that certain security controls related to logical access, physical access, tape encryption, vulnerability management, configuration management, user authentication, and logging and monitoring need improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising Department data and IT resources. However, we have notified appropriate Department management of the specific issues.

Without appropriate security controls related to logical access, physical access, tape encryption, vulnerability management, configuration management, user authentication, and logging and monitoring, the risk is increased that the confidentiality, integrity, and availability of Department data and IT resources may be compromised.

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.

OBJECTIVES, SCOPE, AND METHODOLOGY

The Auditor General conducts operational audits of governmental entities to provide the Legislature, Florida's citizens, public entity management, and other stakeholders unbiased, timely, and relevant information for use in promoting government accountability and stewardship and improving government operations.

We conducted this IT operational audit from December 2019 through August 2020 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for the audit findings and our conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for the audit findings and our conclusions based on our audit objectives.

This IT operational audit focused on evaluating selected significant IT general controls applicable to Department of Agriculture and Consumer Services (Department) operations during the period July 2019 through March 2020 and selected actions prior and subsequent thereto. For those areas addressed by this audit, our audit objectives were:

- To determine the effectiveness of selected significant IT controls in achieving management's objectives in the categories of compliance with controlling laws, administrative rules, and other guidelines; the confidentiality, integrity, availability, relevance, and reliability of data; and the safeguarding of IT resources.
- To identify statutory and fiscal changes that may be recommended to the Legislature pursuant to Section 11.45(7)(h), Florida Statutes.

In planning and conducting our audit, we identified internal controls significant to our audit objectives by considering the internal control integrated framework established by the Committee of Sponsoring

Organizations (COSO)[12] and adapted for a government environment within the *Standards for Internal Control in the Federal Government* issued by the United States Government Accountability Office. That framework is illustrated in the following table.

COSO Internal Control Integrated Framework

Internal Control Component	Description	Underlying Principles (To be Applied by Department Management)
Control Environment	Standards, processes, and structures that provide the basis for carrying out internal control across the organization. Represents the foundation on which an effective internal control system is built.	• Demonstrate commitment to integrity and ethical values. • Exercise oversight responsibility. • Establish structures and reporting lines and assign authorities and responsibilities. • Demonstrate commitment to a competent workforce. • Hold individuals accountable for their responsibilities.
Risk Assessment	Management's process to consider the impact of possible changes in the internal and external environment and to consider actions to mitigate the impact. The basis for how risks will be managed.	• Establish clear objectives to define risk and risk tolerances. • Identify, analyze, and respond to risks. • Consider the potential for fraud. • Identify, analyze, and respond to significant changes that impact the internal control system.
Control Activities	Activities in the form of policies, procedures, and standards that help management mitigate risks. Control activities may be preventive in nature or detective in nature and may be performed at all levels of the organization.	• Design control activities to achieve objectives and respond to risks. • Design control activities over technology. • Implement control activities through policies and procedures.
Information and Communication	Information obtained or generated by management to support the internal control system. Communication is the dissemination of important information to help the organization meet requirements and expectations.	• Use relevant and quality information. • Communicate necessary information internally to achieve entity objectives. • Communicate necessary information externally to achieve entity objectives.
Monitoring	Periodic or ongoing evaluations to verify that the internal control system is present and functioning properly.	• Conduct periodic or ongoing evaluations of the internal control system. • Remediate identified internal control deficiencies on a timely basis.

We determined that all internal control components were significant to our audit objectives. The associated underlying principles significant to our objectives included:

- Management commitment to integrity and ethical values.
- Management establishment of an organizational structure, assignment of responsibility, and delegation of authority to achieve the Department's goals and objectives.
- Management establishment of clear objectives to enable the identification of risks and define risk tolerances.
- Management identification and analysis of and response to risks.
- Management design of control activities to achieve the Department's objectives and respond to risks.
- Management design of controls over information technology.
- Management establishment of policies and procedures to implement internal control activities.
- Management use of relevant and quality information to achieve the Department's objectives.

[12] The Committee of Sponsoring Organizations (COSO) of the Treadway Commission was established in 1985 to develop guidance in the areas of risk and control which enable good organizational governance and reduction of fraud. Pursuant to their mission, COSO developed a framework for internal control that consists of five components and 17 underlying principles.

- Management communication of information internally necessary to achieve the Department's objectives.
- Management activities to monitor the Department's internal control system and evaluate the results.
- Management remediation of identified internal control deficiencies on a timely basis.

This audit was designed to identify, for the IT systems and controls included within the scope of the audit, deficiencies in management's internal controls that were significant to our audit objectives; instances of noncompliance with applicable governing laws, rules, or contracts; and instances of inefficient or ineffective operational policies, procedures, or practices. The focus of this audit was to identify problems so that they may be corrected in such a way as to improve government accountability and efficiency and the stewardship of management. Professional judgment has been used in determining significance and audit risk and in selecting the particular IT controls, legal compliance matters, and records considered.

As described in more detail below, for the IT systems and controls included within the scope of this audit, our audit work included, but was not limited to, communicating to management and those charged with governance the scope, objectives, timing, overall methodology, and reporting of the audit; obtaining an understanding of and evaluating the IT systems and related significant controls; exercising professional judgment in considering significance and audit risk in the design and execution of the research, interviews, tests, analyses, and other procedures included in the audit methodology; obtaining reasonable assurance of the overall sufficiency and appropriateness of the evidence gathered in support of the audit findings and our conclusions; and reporting on the results of the audit as required by governing laws and auditing standards.

This audit included the selection and examination of IT system controls and records. Unless otherwise indicated in this report, these items were not selected with the intent of statistically projecting the results, although we have presented for perspective, where practicable, information concerning relevant population value or size and quantifications relative to the items selected for examination.

An audit by its nature does not include a review of all records and actions of agency management, staff, and contractors and, as a consequence, cannot be relied upon to identify all instances of noncompliance, fraud, abuse, or inefficiency.

In conducting this audit, we:

- Reviewed applicable laws, rules, Department policies and procedures, and other guidelines and interviewed Department personnel to obtain an understanding of selected Department IT general controls.
- Interviewed Department personnel and examined Department records to obtain an understanding of the Department network infrastructure and related hardware and software; processes for intrusion detection and prevention; vulnerability management, including vulnerability testing, analysis, and remediation; security awareness training; and restricting, assigning, logging, and reviewing physical access to sensitive IT resources.
- Interviewed Department personnel and examined Department records to assess the adequacy of Department IT asset controls for managing Department servers and high-risk network devices.
- Interviewed Department personnel and examined Department records to determine whether the Information Security Manager (ISM) reported directly to the Commissioner for the purposes of the ISM's information security duties as required by Section 282.318, Florida Statutes.

- Interviewed Department personnel, reviewed Department policies and procedures, and examined Department computer security incident response records to determine whether the Department complied with Department of Management Services Rule 60GG-2.005(1)(a), Florida Administrative Code, for establishing and maintaining incident response processes and procedures to ensure timely responses for detected cybersecurity incidents.
- Interviewed Department and Division personnel and examined Department and Division records to assess the adequacy of disaster recovery controls, including policies and procedures, disaster recovery plans, and disaster recovery plan testing, and whether such controls facilitated the timely and orderly resumption of IT resources in the event of a disaster.
- Interviewed Department and Division personnel and examined Department and Division records to determine whether recoverability testing of backup media was performed and documented, backup media was adequately protected and securely stored off-site, and server backups were timely performed. Specifically, to determine whether backups were timely performed, we evaluated backup server reports as of January 30, 2020, for:
    - 44 of the 307 Department-managed Windows and Linux production servers.
    - The 9 Division-managed Windows production servers.
    - The 12 Department-managed Oracle Solaris production servers.
- Interviewed Department personnel and evaluated Department policies, procedures, and processes for security awareness training. Specifically, we evaluated Department training records for:
    - 35 of the 256 employees hired during the period July 2019 through December 2019 to determine whether the selected employees completed the required new hire security awareness training within 30 days of hire.
    - 35 selected employees hired prior to March 27, 2019, from the population of 2,968 employees as of February 21, 2020, to determine whether the selected employees timely completed annual security awareness training.
    - 20 selected Other Personal Services (OPS) employees hired prior to January 1, 2020, from the population of 507 OPS employees as of February 20, 2020, to determine whether the selected OPS employees timely completed security awareness training.
- Interviewed Department personnel and evaluated Department policies, procedures, and processes for assigning and periodically reviewing administrative access to high-risk network devices and the Department network domain. Specifically, we evaluated the appropriateness of:
    - The 29 local administrative accounts as of December 19, 2019, for nine high-risk network devices and the 3 local administrative accounts as of February 21, 2020, for another high-risk network device.
    - The 21 administrative network service accounts and 14 administrative network user accounts as of December 12, 2019, with membership in the *Enterprise Admins*, *Schema Admins*, *Domain Admins*, or *Administrators* security groups.
- Interviewed Department personnel and examined Department policies, procedures, and processes for authorizing, removing, periodically reviewing, and logging physical access to the Department data center and backup media storage locations, including evaluating the appropriateness of the 32 active users as of January 7, 2020, with access to the data center.
- Evaluated the adequacy of Department vulnerability management controls, including the sufficiency of policies and procedures, timely performance of authenticated scans, and timely communication, analysis, and remediation of identified vulnerabilities.

- Evaluated the adequacy of Department configuration management policies, procedures, and processes for ensuring that patches for high-risk network devices and servers were timely analyzed and applied as necessary. Specifically, we evaluated:
    - 12 high-risk network devices, as of December 19, 2019, February 21, 2020, and March 8, 2020, to determine whether operating systems were supported and up to date.
    - The 275 Department-managed and the 36 Division-managed Windows servers to determine whether the server operating systems were supported by the vendor as of January 17, 2020.
    - 28 of the 263 vendor-supported and Department-managed production servers operating systems to determine whether the server operating systems were up to date as of February 28, 2020, and whether monthly security patches were applied during the period July 2019 through January 2020.
    - 15 of the 32 vendor-supported and Division-managed production server operating systems to determine whether the server operating systems were up to date as of February 20, 2020, for 13 servers, and February 28, 2020, for 2 servers and whether monthly security patches were applied during the period July 2019 through January 2020.
    - The 6 open-system production server operating systems to determine whether the server operating systems were supported by the vendor as of February 18, 2020.
- Evaluated the adequacy of authentication controls, including policies and procedures and authentication settings, for the Department network domain and high-risk network devices.
- Evaluated the adequacy of selected Department and Division logging and monitoring controls.
- Communicated on an interim basis with applicable officials to ensure the timely resolution of issues involving controls and noncompliance.
- Performed various other auditing procedures, including analytical procedures, as necessary, to accomplish the objectives of the audit.
- Prepared and submitted for management response the findings and recommendations that are included in this report and which describe the matters requiring corrective actions. Management's response is included in this report under the heading ***MANAGEMENT'S RESPONSE***.

AUTHORITY

Section 11.45, Florida Statutes, provides that the Auditor General may conduct audits of the IT programs, activities, functions, or systems of any governmental entity created or established by law. Pursuant to the provisions of Section 11.45, Florida Statutes, I have directed that this report be prepared to present the results of our IT operational audit.

Sherrill F. Norman, CPA
Auditor General

OFFICE OF THE COMMISSIONER
(850) 617-7700

THE CAPITOL
400 SOUTH MONROE STREET
TALLAHASSEE, FLORIDA 32399-0800

FLORIDA DEPARTMENT OF AGRICULTURE AND CONSUMER SERVICES
COMMISSIONER NICOLE "NIKKI" FRIED

June 16, 2021

Ms. Sherrill F. Norman, CPA
Auditor General, State of Florida
G74 Claude Pepper Building
111 West Madison Street
Tallahassee, Florida 32399-1450

Dear Ms. Norman:

Thank you for the opportunity to respond to the preliminary and tentative audit findings and recommendations for the Auditor General's information technology (IT) operational audit of the Department of Agriculture and Consumer Services' General Controls. Our responses are documented below.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

I appreciate your staff's efforts in helping to improve our IT controls.

Sincerely,

Nicole Fried
Commissioner of Agriculture