By Senator Hooper

16-01145-19 20191570__

A bill to be entitled

An act relating to information technology reorganization; transferring all powers, duties, functions, records, offices, personnel, associated administrative support positions, property, pending issues and existing contracts, administrative authority, certain administrative rules, trust funds, and unexpended balances of appropriations, allocations, and other funds of the Agency for State Technology to the Department of Management Services by a type two transfer; providing for the continuation of certain contracts and interagency agreements; amending s. 20.22, F.S.; establishing the Division of State Technology within the Department of Management Services to supersede the Technology Program; establishing the position of state chief information officer and providing qualifications thereof; amending s. 20.255, F.S.; removing the expiration for provisions designating the Department of Environmental Protection as the lead agency for geospatial data; authorizing the department to adopt rules for specified purposes; repealing s. 20.61, F.S., relating to the Agency for State Technology; amending s. 112.061, F.S.; authorizing the Department of Management Services to adopt rules for certain purposes; defining the term "statewide travel management system"; specifying reporting requirements for executive branch agencies and the judicial branch through the statewide travel management system;

specifying that travel reports on the system may not reveal confidential or exempt information; amending s. 282.003, F.S.; revising a short title; reordering and amending s. 282.0041, F.S.; revising and providing definitions; amending s. 282.0051, F.S.; transferring powers, duties, and functions of the Agency for State Technology to the Department of Management Services and revising such powers, duties, and functions; removing certain project oversight requirements; requiring agency projected costs for data center services to be provided to the Governor and the Legislature on an annual basis; requiring the department to provide certain recommendations; amending s. 282.201, F.S.; transferring the state data center from the Agency for State Technology to the Department of Management Services; requiring the department to appoint a director of the state data center; deleting legislative intent; revising duties of the state data center; requiring the state data center to show preference for cloud-computing solutions in its procurement process; revising the use of the state data center and certain consolidation requirements; removing obsolete language; revising agency limitations; creating s. 282.206, F.S.; providing legislative intent regarding the use of cloud computing; requiring each state agency to adopt formal procedures for cloud-computing options; requiring a state agency to develop, and update annually, a strategic plan for submission to the

Governor and the Legislature; specifying requirements for the strategic plan; requiring a state agency customer entity to notify the state data center biannually of changes in anticipated use of state data center services; specifying requirements and limitations as to cloud-computing services for the Department of Law Enforcement; amending s. 282.318, F.S.; requiring the Department of Management Services to appoint a state chief information security officer; revising and specifying requirements for service-level agreements for information technology and information technology resources and services; conforming provisions to changes made by the act; amending ss. 17.0315, 20.055, 97.0525, 110.205, 215.322, 215.96, 287.057, 282.00515, 287.0591, 365.171, 365.172, 365.173, 445.011, 445.045, 668.50, and 943.0415, F.S.; conforming provisions and a cross-reference to changes made by the act; creating the Florida Cybersecurity Task Force; providing for the membership, meeting requirements, and duties of the task force; providing for administrative and staff support; requiring executive branch departments and agencies to cooperate with information requests made by the task force; providing reporting requirements; providing for expiration of the task force; providing an effective date.

Be It Enacted by the Legislature of the State of Florida:

Section 1. All powers; duties; functions; records; offices; personnel; associated administrative support positions; property; pending issues and existing contracts; administrative authority; administrative rules in chapter 74, Florida Administrative Code, in effect as of July 1, 2019; trust funds; and unexpended balances of appropriations, allocations, and other funds of the Agency for State Technology are transferred by a type two transfer pursuant to s. 20.06(2), Florida Statutes, to the Department of Management Services.

Section 2. Any contract or interagency agreement existing before July 1, 2019, between the Agency for State Technology, or any entity or agent of the agency, and any other agency, entity, or person shall continue as a contract or agreement on the successor department or entity responsible for the program, activity, or function relative to the contract or agreement.

Section 3. Paragraph (b) of subsection (2) and subsection (4) of section 20.22, Florida Statutes, are amended to read:

20.22 Department of Management Services.—There is created a Department of Management Services.

(2) The following divisions and programs within the Department of Management Services are established:

(b) Division of State Technology, the director of which is appointed by the secretary of the department and shall serve as the state chief information officer. The state chief information officer must be a proven, effective administrator who must have at least 10 years of executive-level experience in the public or private sector, preferably with experience in the development of information technology strategic planning and the development and implementation of fiscal and substantive information

technology policy and standards ~~Technology Program~~.

~~(4) The Department of Management Services shall provide the Agency for State Technology with financial management oversight. The agency shall provide the department all documents and necessary information, as requested, to meet the requirements of this section. The department's financial management oversight includes:~~

~~(a) Developing and implementing cost-recovery mechanisms for the administrative and data center costs of services through agency assessments of applicable customer entities. Such cost-recovery mechanisms must comply with applicable state and federal regulations concerning the distribution and use of funds and must ensure that, for each fiscal year, no service or customer entity subsidizes another service or customer entity.~~

~~(b) Implementing an annual reconciliation process to ensure that each customer entity is paying for the full direct and indirect cost of each service as determined by the customer entity's use of each service.~~

~~(c) Providing rebates that may be credited against future billings to customer entities when revenues exceed costs.~~

~~(d) Requiring each customer entity to transfer sufficient funds into the appropriate data processing appropriation category before implementing a customer entity's request for a change in the type or level of service provided, if such change results in a net increase to the customer entity's costs for that fiscal year.~~

~~(e) By October 1, 2018, providing to each customer entity's agency head the estimated agency assessment cost by the Agency for State Technology for the following fiscal year. The agency~~

~~assessment cost of each customer entity includes administrative and data center services costs of the agency.~~

~~(f) Preparing the legislative budget request for the Agency for State Technology based on the issues requested and approved by the executive director of the Agency for State Technology. Upon the approval of the agency's executive director, the Department of Management Services shall transmit the agency's legislative budget request to the Governor and the Legislature pursuant to s. 216.023.~~

~~(g) Providing a plan for consideration by the Legislative Budget Commission if the Agency for State Technology increases the cost of a service for a reason other than a customer entity's request made under paragraph (d). Such a plan is required only if the service cost increase results in a net increase to a customer entity.~~

~~(h) Providing a timely invoicing methodology to recover the cost of services provided to the customer entity pursuant to s. 215.422.~~

~~(i) Providing an annual reconciliation process of prior year expenditures completed on a timely basis and overall budget management pursuant to chapter 216.~~

~~(j) This subsection expires July 1, 2019.~~

Section 4. Subsection (9) of section 20.255, Florida Statutes, is amended to read:

20.255 Department of Environmental Protection.—There is created a Department of Environmental Protection.

(9) The department shall act as the lead agency of the executive branch for the development and review of policies, practices, and standards related to geospatial data <u>managed by</u>

state agencies and water management districts. The department shall coordinate and promote geospatial data sharing throughout ~~the~~ state government and serve as the primary point of contact for statewide geographic information systems projects, grants, and resources. The department may adopt rules pursuant to ss. 120.536(1) and 120.54 to implement this subsection ~~This subsection expires July 1, 2019~~.

Section 5. Section 20.61, Florida Statutes, is repealed.

Section 6. Paragraph (c) is added to subsection (9) of section 112.061, Florida Statutes, and subsection (16) is added to that section, to read:

112.061 Per diem and travel expenses of public officers, employees, and authorized persons; statewide travel management system.—

(9) RULES.—

(c) The Department of Management Services may adopt rules to administer the provisions of this section which relate to the statewide travel management system.

(16) STATEWIDE TRAVEL MANAGEMENT SYSTEM.—

(a) For purposes of this subsection, "statewide travel management system" means the system developed by the Department of Management Services to:

1. Collect and store information relating to public officer or employee travel information;

2. Standardize and automate agency travel management;

3. Allow for travel planning and approval, expense reporting, and reimbursement; and

4. Allow travel information queries.

(b) Each executive branch state government agency and the

judicial branch must report on the statewide travel management system all public officer and employee travel information, including, but not limited to, name and position title; purpose of travel; dates and location of travel; mode of travel; confirmation from the head of the agency or designee authorization, if required; and total travel cost. Each executive branch state government agency and the judicial branch must use the statewide travel management system for purposes of travel authorization and reimbursement.

(c) Travel reports made available on the statewide travel management system may not reveal information made confidential or exempt by law.

Section 7. Section 282.003, Florida Statutes, is amended to read:

282.003 Short title.—This part may be cited as the "~~Enterprise~~ Information Technology ~~Services~~ Management Act."

Section 8. Effective July 1, 2019, and upon the expiration of the amendment to that section made by chapter 2018-10, Laws of Florida, section 282.0041, Florida Statutes, is reordered and amended to read:

282.0041 Definitions.—As used in this chapter, the term:

(1) "Agency assessment" means the amount each customer entity must pay annually for services from the Department of Management Services and includes administrative and data center services costs.

(2) ~~(1)~~ "Agency data center" means agency space containing 10 or more physical or logical servers.

(3) ~~(2)~~ "Breach" has the same meaning as provided in s. 501.171 ~~means a confirmed event that compromises the~~

~~confidentiality, integrity, or availability of information or data~~.

(4)~~(3)~~ "Business continuity plan" means a collection of procedures and information designed to keep an agency's critical operations running during a period of displacement or interruption of normal operations.

(5) "Cloud computing" has the same meaning as provided in Special Publication 800-145 issued by the National Institute of Standards and Technology.

(6)~~(4)~~ "Computing facility" or "agency computing facility" means agency space containing fewer than a total of 10 physical or logical servers, but excluding single, logical-server installations that exclusively perform a utility function such as file and print servers.

(7)~~(5)~~ "Customer entity" means an entity that obtains services from the Department of Management Services ~~state data center~~.

(8) "Data" means a subset of structured information in a format that allows such information to be electronically retrieved and transmitted.

(9)~~(6)~~ "Department" means the Department of Management Services.

(10)~~(7)~~ "Disaster recovery" means the process, policies, procedures, and infrastructure related to preparing for and implementing recovery or continuation of an agency's vital technology infrastructure after a natural or human-induced disaster.

(11)~~(8)~~ "Enterprise information technology service" means an information technology service that is used in all agencies

or a subset of agencies and is established in law to be designed, delivered, and managed at the enterprise level.

(12)~~(9)~~ "Event" means an observable occurrence in a system or network.

(13)~~(10)~~ "Incident" means a violation or imminent threat of violation, whether such violation is accidental or deliberate, of information technology resources, security ~~policies~~, ~~acceptable use~~ policies, or ~~standard security~~ practices. An imminent threat of violation refers to a situation in which the state agency has a factual basis for believing that a specific incident is about to occur.

(14)~~(11)~~ "Information technology" means equipment, hardware, software, firmware, programs, systems, networks, infrastructure, media, and related material used to automatically, electronically, and wirelessly collect, receive, access, transmit, display, store, record, retrieve, analyze, evaluate, process, classify, manipulate, manage, assimilate, control, communicate, exchange, convert, converge, interface, switch, or disseminate information of any kind or form.

(15)~~(12)~~ "Information technology policy" means a definite course or method of action selected from among one or more alternatives that guide and determine present and future decisions.

(16)~~(13)~~ "Information technology resources" has the same meaning as provided in s. 119.011.

(17)~~(14)~~ "Information technology security" means the protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of data, information, and

information technology resources.

(18) "Open data" means data collected or created by a state agency and structured in a way that enables the data to be fully discoverable and usable by the public. The term does not include data that are restricted from public distribution based on federal or state privacy, confidentiality, and security laws and regulations or data for which a state agency is statutorily authorized to assess a fee for its distribution.

(19)~~(15)~~ "Performance metrics" means the measures of an organization's activities and performance.

(20)~~(16)~~ "Project" means an endeavor that has a defined start and end point; is undertaken to create or modify a unique product, service, or result; and has specific objectives that, when attained, signify completion.

(21)~~(17)~~ "Project oversight" means an independent review and analysis of an information technology project that provides information on the project's scope, completion timeframes, and budget and that identifies and quantifies issues or risks affecting the successful and timely completion of the project.

(22)~~(18)~~ "Risk assessment" means the process of identifying security risks, determining their magnitude, and identifying areas needing safeguards.

(23)~~(19)~~ "Service level" means the key performance indicators (KPI) of an organization or service which must be regularly performed, monitored, and achieved.

(24)~~(20)~~ "Service-level agreement" means a written contract between the Department of Management Services ~~state data center~~ and a customer entity which specifies the scope of services provided, service level, the duration of the agreement, the

responsible parties, and service costs. A service-level agreement is not a rule pursuant to chapter 120.

(25)~~(21)~~ "Stakeholder" means a person, group, organization, or state agency involved in or affected by a course of action.

(26)~~(22)~~ "Standards" means required practices, controls, components, or configurations established by an authority.

(27)~~(23)~~ "State agency" means any official, officer, commission, board, authority, council, committee, or department of the executive branch of state government; the Justice Administrative Commission; and the Public Service Commission. The term does not include university boards of trustees or state universities. As used in part I of this chapter, except as otherwise specifically provided, the term does not include the Department of Legal Affairs, the Department of Agriculture and Consumer Services, or the Department of Financial Services.

(28)~~(24)~~ "SUNCOM Network" means the state enterprise telecommunications system that provides all methods of electronic or optical telecommunications beyond a single building or contiguous building complex and used by entities authorized as network users under this part.

(29)~~(25)~~ "Telecommunications" means the science and technology of communication at a distance, including electronic systems used in the transmission or reception of information.

(30)~~(26)~~ "Threat" means any circumstance or event that has the potential to adversely impact a state agency's operations or assets through an information system via unauthorized access, destruction, disclosure, or modification of information or denial of service.

(31)~~(27)~~ "Variance" means a calculated value that

illustrates how far positive or negative a projection has deviated when measured against documented estimates within a project plan.

Section 9. Effective July 1, 2019, and upon the expiration of the amendment to that section made by chapter 2018-10, Laws of Florida, section 282.0051, Florida Statutes, is amended to read:

282.0051 Department of Management Services ~~Agency for State Technology~~; powers, duties, and functions.—The department ~~Agency for State Technology~~ shall have the following powers, duties, and functions:

(1) Develop and publish information technology policy for the management of the state's information technology resources.

(2) Establish and publish information technology architecture standards to provide for the most efficient use of the state's information technology resources and to ensure compatibility and alignment with the needs of state agencies. The department ~~agency~~ shall assist state agencies in complying with the standards.

(3) ~~By June 30, 2015,~~ Establish project management and oversight standards with which state agencies must comply when implementing information technology projects. The department ~~agency~~ shall provide training opportunities to state agencies to assist in the adoption of the project management and oversight standards. To support data-driven decisionmaking, the standards must include, but are not limited to:

(a) Performance measurements and metrics that objectively reflect the status of an information technology project based on a defined and documented project scope, cost, and schedule.

(b) Methodologies for calculating acceptable variances in the projected versus actual scope, schedule, or cost of an information technology project.

(c) Reporting requirements, including requirements designed to alert all defined stakeholders that an information technology project has exceeded acceptable variances defined and documented in a project plan.

(d) Content, format, and frequency of project updates.

(4) ~~Beginning January 1, 2015,~~ Perform project oversight on all state agency information technology projects that have total project costs of $10 million or more and that are funded in the General Appropriations Act or any other law. The department ~~agency~~ shall report at least quarterly to the Executive Office of the Governor, the President of the Senate, and the Speaker of the House of Representatives on any information technology project that the department ~~agency~~ identifies as high-risk due to the project exceeding acceptable variance ranges defined and documented in a project plan. The report must include a risk assessment, including fiscal risks, associated with proceeding to the next stage of the project, and a recommendation for corrective actions required, including suspension or termination of the project.

(5) ~~By April 1, 2016, and biennially thereafter,~~ Identify opportunities for standardization and consolidation of information technology services that support business functions and operations, including administrative functions such as purchasing, accounting and reporting, cash management, and personnel, and that are common across state agencies. The department ~~agency~~ shall biennially on April 1 provide

recommendations for standardization and consolidation to the Executive Office of the Governor, the President of the Senate, and the Speaker of the House of Representatives. ~~The agency is not precluded from providing recommendations before April 1, 2016.~~

(6) ~~In collaboration with the Department of Management Services,~~ Establish best practices for the procurement of information technology products and cloud-computing services in order to reduce costs, increase the quality of data center services ~~productivity~~, or improve government services. ~~Such practices must include a provision requiring the agency to review all information technology purchases made by state agencies that have a total cost of $250,000 or more, unless a purchase is specifically mandated by the Legislature, for compliance with the standards established pursuant to this section.~~

(7) ~~(a) Participate with the Department of Management Services in evaluating, conducting, and negotiating competitive solicitations for state term contracts for information technology commodities, consultant services, or staff augmentation contractual services pursuant to s. 287.0591.~~

~~(b) Collaborate with the Department of Management Services in information technology resource acquisition planning.~~

~~(8)~~ Develop standards for information technology reports and updates, including, but not limited to, operational work plans, project spend plans, and project status reports, for use by state agencies.

(8) ~~(9)~~ Upon request, assist state agencies in the development of information technology-related legislative budget

requests.

(9) ~~(10) Beginning July 1, 2016, and annually thereafter,~~ Conduct annual assessments of state agencies to determine compliance with all information technology standards and guidelines developed and published by the department ~~agency, and beginning December 1, 2016, and annually thereafter,~~ and provide results of the assessments to the Executive Office of the Governor, the President of the Senate, and the Speaker of the House of Representatives.

(10)~~(11)~~ Provide operational management and oversight of the state data center established pursuant to s. 282.201, which includes:

(a) Implementing industry standards and best practices for the state data center's facilities, operations, maintenance, planning, and management processes.

(b) Developing and implementing cost-recovery mechanisms that recover the full direct and indirect cost of services through charges to applicable customer entities. Such cost-recovery mechanisms must comply with applicable state and federal regulations concerning distribution and use of funds and must ensure that, for any fiscal year, no service or customer entity subsidizes another service or customer entity.

(c) Developing and implementing appropriate operating guidelines and procedures necessary for the state data center to perform its duties pursuant to s. 282.201. The guidelines and procedures must comply with applicable state and federal laws, regulations, and policies and conform to generally accepted governmental accounting and auditing standards. The guidelines and procedures must include, but need not be limited to:

1. Implementing a consolidated administrative support structure responsible for providing financial management, procurement, transactions involving real or personal property, human resources, and operational support.

2. Implementing an annual reconciliation process to ensure that each customer entity is paying for the full direct and indirect cost of each service as determined by the customer entity's use of each service.

3. Providing rebates that may be credited against future billings to customer entities when revenues exceed costs.

4. Requiring customer entities to validate that sufficient funds exist in the appropriate data processing appropriation category or will be transferred into the appropriate data processing appropriation category before implementation of a customer entity's request for a change in the type or level of service provided, if such change results in a net increase to the customer entity's cost for that fiscal year.

5. By November 15 ~~September 1~~ of each year, providing to the Office of Policy and Budget in the Executive Office of the Governor and to the chairs of the legislative appropriations committees ~~each customer entity's agency head~~ the projected costs of providing data center services for the following fiscal year.

6. Providing a plan for consideration by the Legislative Budget Commission if the cost of a service is increased for a reason other than a customer entity's request made pursuant to subparagraph 4. Such a plan is required only if the service cost increase results in a net increase to a customer entity for that fiscal year.

7. Standardizing and consolidating procurement and contracting practices.

(d) In collaboration with the Department of Law Enforcement, developing and implementing a process for detecting, reporting, and responding to information technology security incidents, breaches, and threats.

(e) Adopting rules relating to the operation of the state data center, including, but not limited to, budgeting and accounting procedures, cost-recovery methodologies, and operating procedures.

(f) ~~Beginning May 1, 2016, and annually thereafter,~~ Conducting an annual ~~a~~ market analysis to determine whether the state's approach to the provision of data center services is the most effective and cost-efficient ~~efficient~~ manner by which its customer entities can acquire such services, based on federal, state, and local government trends; best practices in service provision; and the acquisition of new and emerging technologies. The results of the market analysis shall assist the state data center in making adjustments to its data center service offerings.

(11) ~~(12)~~ Recommend other information technology services that should be designed, delivered, and managed as enterprise information technology services. Recommendations must include the identification of existing information technology resources associated with the services, if existing services must be transferred as a result of being delivered and managed as enterprise information technology services.

~~(13) Recommend additional consolidations of agency computing facilities or data centers into the state data center~~

~~established pursuant to s. 282.201. Such recommendations shall include a proposed timeline for consolidation.~~

(12)~~(14)~~ In consultation with state agencies, propose a methodology and approach for identifying and collecting both current and planned information technology expenditure data at the state agency level.

(13)(a) ~~(15)(a) Beginning January 1, 2015, and~~ Notwithstanding any other law, provide project oversight on any information technology project of the Department of Financial Services, the Department of Legal Affairs, and the Department of Agriculture and Consumer Services which ~~that~~ has a total project cost of $25 million or more and which ~~that~~ impacts one or more other agencies. Such information technology projects must also comply with the applicable information technology architecture, project management and oversight, and reporting standards established by the department ~~agency~~.

(b) When performing the project oversight function specified in paragraph (a), report at least quarterly to the Executive Office of the Governor, the President of the Senate, and the Speaker of the House of Representatives on any information technology project that the department ~~agency~~ identifies as high-risk due to the project exceeding acceptable variance ranges defined and documented in the project plan. The report shall include a risk assessment, including fiscal risks, associated with proceeding to the next stage of the project and a recommendation for corrective actions required, including suspension or termination of the project.

(14)~~(16)~~ If an information technology project implemented by a state agency must be connected to or otherwise accommodated

by an information technology system administered by the Department of Financial Services, the Department of Legal Affairs, or the Department of Agriculture and Consumer Services, consult with these departments regarding the risks and other effects of such projects on their information technology systems and work cooperatively with these departments regarding the connections, interfaces, timing, or accommodations required to implement such projects.

(15) ~~(17)~~ If adherence to standards or policies adopted by or established pursuant to this section causes conflict with federal regulations or requirements imposed on a state agency and results in adverse action against the state agency or federal funding, work with the state agency to provide alternative standards, policies, or requirements that do not conflict with the federal regulation or requirement. ~~Beginning July 1, 2015,~~ The department ~~agency~~ shall annually report such alternative standards to the Governor, the President of the Senate, and the Speaker of the House of Representatives.

(16) ~~(18) In collaboration with the Department of Management Services:~~

(a) Establish an information technology policy for all information technology-related state contracts, including state term contracts for information technology commodities, consultant services, and staff augmentation services. The information technology policy must include:

1. Identification of the information technology product and service categories to be included in state term contracts.

2. Requirements to be included in solicitations for state term contracts.

3. Evaluation criteria for the award of information technology-related state term contracts.

4. The term of each information technology-related state term contract.

5. The maximum number of vendors authorized on each state term contract.

(b) Evaluate vendor responses for information technology-related state term contract solicitations and invitations to negotiate.

(c) Answer vendor questions on information technology-related state term contract solicitations.

(d) Ensure that the information technology policy established pursuant to paragraph (a) is included in all solicitations and contracts that ~~which~~ are administratively executed by the department.

(17) Recommend potential methods for standardizing data across state agencies which will promote interoperability and reduce the collection of duplicative data.

(18) Recommend open data technical standards and terminologies for use by state agencies.

(19) Adopt rules to administer this section.

Section 10. Effective July 1, 2019, and upon the expiration of the amendment to that section made by chapter 2018-10, Laws of Florida, section 282.201, Florida Statutes, is amended to read:

282.201 State data center.—The state data center is established within the department ~~Agency for State Technology and shall provide data center services that are hosted on premises or externally through a third-party provider as an~~

~~enterprise information technology service~~. The provision of data center services must comply with applicable state and federal laws, regulations, and policies, including all applicable security, privacy, and auditing requirements. The department shall appoint a director of the state data center, preferably an individual who has experience in leading data center facilities and has expertise in cloud-computing management.

~~(1) INTENT.—The Legislature finds that the most efficient and effective means of providing quality utility data processing services to state agencies requires that computing resources be concentrated in quality facilities that provide the proper security, disaster recovery, infrastructure, and staff resources to ensure that the state's data is maintained reliably and safely, and is recoverable in the event of a disaster. Unless otherwise exempt by law, it is the intent of the Legislature that all agency data centers and computing facilities shall be consolidated into the state data center.~~

(1)~~(2)~~ STATE DATA CENTER DUTIES.—The state data center shall:

(a) Offer, develop, and support the services and applications defined in service-level agreements executed with its customer entities.

(b) Maintain performance of the state data center by ensuring proper data backup, data backup recovery, disaster recovery, and appropriate security, power, cooling, fire suppression, and capacity.

(c) Develop and implement ~~a~~ business continuity ~~plan~~ and ~~a~~ disaster recovery plans ~~plan, and beginning July 1, 2015~~, and annually ~~thereafter,~~ conduct a live exercise of each plan.

(d) Enter into a service-level agreement with each customer entity to provide the required type and level of service or services. If a customer entity fails to execute an agreement within 60 days after commencement of a service, the state data center may cease service. A service-level agreement may not have a term exceeding 3 years and at a minimum must:

1. Identify the parties and their roles, duties, and responsibilities under the agreement.

2. State the duration of the contract term and specify the conditions for renewal.

3. Identify the scope of work.

4. Identify the products or services to be delivered with sufficient specificity to permit an external financial or performance audit.

5. Establish the services to be provided, the business standards that must be met for each service, the cost of each service <u>by agency application</u>, and the metrics and processes by which the business standards for each service are to be objectively measured and reported.

6. Provide a timely billing methodology to recover the costs of services provided to the customer entity pursuant to s. 215.422.

7. Provide a procedure for modifying the service-level agreement based on changes in the type, level, and cost of a service.

8. Include a right-to-audit clause to ensure that the parties to the agreement have access to records for audit purposes during the term of the service-level agreement.

9. Provide that a service-level agreement may be terminated

by either party for cause only after giving the other party and the department ~~Agency for State Technology~~ notice in writing of the cause for termination and an opportunity for the other party to resolve the identified cause within a reasonable period.

10. Provide for mediation of disputes by the Division of Administrative Hearings pursuant to s. 120.573.

(e) For purposes of chapter 273, be the custodian of resources and equipment located in and operated, supported, and managed by the state data center.

(f) Assume administrative access rights to resources and equipment, including servers, network components, and other devices, consolidated into the state data center.

1. Upon ~~the date of each~~ consolidation ~~specified in this section, the General Appropriations Act, or any other law~~, a state agency shall relinquish administrative rights to consolidated resources and equipment. State agencies required to comply with federal and state criminal justice information security rules and policies shall retain administrative access rights sufficient to comply with the management control provisions of those rules and policies; however, the state data center shall have the appropriate type or level of rights to allow the center to comply with its duties pursuant to this section. The Department of Law Enforcement shall serve as the arbiter of disputes pertaining to the appropriate type and level of administrative access rights pertaining to the provision of management control in accordance with the federal criminal justice information guidelines.

2. The state data center shall provide customer entities with access to applications, servers, network components, and

other devices necessary for entities to perform business activities and functions, and as defined and documented in a service-level agreement.

(g) In its procurement process, show preference for cloud-computing solutions that minimize or do not require the purchasing, financing, or leasing of state data center infrastructure, and that meet the needs of customer agencies, that reduce costs, and that meet or exceed the applicable state and federal laws, regulations, and standards for information technology security.

(h) Assist customer entities in transitioning from state data center services to third-party cloud-computing services procured by a customer entity.

~~(3) STATE AGENCY DUTIES.—~~

~~(a) Each state agency shall provide to the Agency for State Technology all requested information relating to its data centers and computing facilities and any other information relevant to the effective transition of an agency data center or computing facility into the state data center.~~

~~(b) Each state agency customer of the state data center shall notify the state data center, by May 31 and November 30 of each year, of any significant changes in anticipated utilization of state data center services pursuant to requirements established by the state data center.~~

(2) ~~(4)~~ USE OF THE STATE DATA CENTER ~~SCHEDULE FOR CONSOLIDATIONS OF AGENCY DATA CENTERS~~.—

~~(a) Consolidations of agency data centers and computing facilities into the state data center shall be made by the dates specified in this section and in accordance with budget~~

~~adjustments contained in the General Appropriations Act.~~

~~(b) During the 2013-2014 fiscal year, the following state agencies shall be consolidated by the specified date:~~

~~1. By October 31, 2013, the Department of Economic Opportunity.~~

~~2. By December 31, 2013, the Executive Office of the Governor, to include the Division of Emergency Management except for the Emergency Operation Center's management system in Tallahassee and the Camp Blanding Emergency Operations Center in Starke.~~

~~3. By March 31, 2014, the Department of Elderly Affairs.~~

~~4. By October 30, 2013, the Fish and Wildlife Conservation Commission, except for the commission's Fish and Wildlife Research Institute in St. Petersburg.~~

~~(c)~~ The following are exempt from the use of the state data center ~~consolidation under this section~~: the Department of Law Enforcement, the Department of the Lottery's Gaming System, Systems Design and Development in the Office of Policy and Budget, the regional traffic management centers as described in s. 335.14(2) and the Office of Toll Operations of the Department of Transportation, the State Board of Administration, state attorneys, public defenders, criminal conflict and civil regional counsel, capital collateral regional counsel, and the Florida Housing Finance Corporation.

~~(d) A state agency that is consolidating its agency data center or computing facility into the state data center must execute a new or update an existing service-level agreement within 60 days after the commencement of the service. If a state agency and the state data center are unable to execute a~~

~~service-level agreement by that date, the agency shall submit a report to the Executive Office of the Governor within 5 working days after that date which explains the specific issues preventing execution and describing the plan and schedule for resolving those issues.~~

~~(c) Each state agency scheduled for consolidation into the state data center shall submit a transition plan to the Agency for State Technology by July 1 of the fiscal year before the fiscal year in which the scheduled consolidation will occur. Transition plans shall be developed in consultation with the state data center and must include:~~

~~1. An inventory of the agency data center's resources being consolidated, including all hardware and its associated life cycle replacement schedule, software, staff, contracted services, and facility resources performing data center management and operations, security, backup and recovery, disaster recovery, system administration, database administration, system programming, job control, production control, print, storage, technical support, help desk, and managed services, but excluding application development, and the agency's costs supporting these resources.~~

~~2. A list of contracts in effect, including, but not limited to, contracts for hardware, software, and maintenance, which identifies the expiration date, the contract parties, and the cost of each contract.~~

~~3. A detailed description of the level of services needed to meet the technical and operational requirements of the platforms being consolidated.~~

~~4. A timetable with significant milestones for the~~

~~completion of the consolidation.~~

~~(f) Each state agency scheduled for consolidation into the state data center shall submit with its respective legislative budget request the specific recurring and nonrecurring budget adjustments of resources by appropriation category into the appropriate data processing category pursuant to the legislative budget request instructions in s. 216.023.~~

(3)~~(5)~~ AGENCY LIMITATIONS.—

~~(a)~~ Unless exempt from the use of the state data center ~~consolidation~~ pursuant to this section or authorized by the Legislature ~~or as provided in paragraph (b)~~, a state agency may not:

(a)~~1.~~ Create a new agency computing facility or data center, or expand the capability to support additional computer equipment in an existing agency computing facility or data center; or

~~2. Spend funds before the state agency's scheduled consolidation into the state data center to purchase or modify hardware or operations software that does not comply with standards established by the Agency for State Technology pursuant to s. 282.0051;~~

~~3. Transfer existing computer services to any data center other than the state data center;~~

(b)~~4.~~ Terminate services with the state data center without giving written notice of intent to terminate services 180 days before such termination~~; or~~

~~5. Initiate a new computer service except with the state data center.~~

~~(b) Exceptions to the limitations in subparagraphs (a)1.,~~

~~2., 3., and 5. may be granted by the Agency for State Technology if there is insufficient capacity in the state data center to absorb the workload associated with agency computing services, if expenditures are compatible with the standards established pursuant to s. 282.0051, or if the equipment or resources are needed to meet a critical agency business need that cannot be satisfied by the state data center. The Agency for State Technology shall establish requirements that a state agency must follow when submitting and documenting a request for an exception. The Agency for State Technology shall also publish guidelines for its consideration of exception requests. However, the decision of the Agency for State Technology regarding an exception request is not subject to chapter 120~~.

Section 11. Section 282.206, Florida Statutes, is created to read:

282.206 Cloud-first policy in state agencies.—

(1) The Legislature finds that the most efficient and effective means of providing quality data processing services is through the use of cloud computing. It is the intent of the Legislature that each state agency adopt a cloud-first policy that first considers cloud-computing solutions in its technology sourcing strategy for technology initiatives or upgrades whenever possible and feasible.

(2) In its procurement process, each state agency shall show a preference for cloud-computing solutions that either minimize or do not require the use of state data center infrastructure when cloud-computing solutions meet the needs of the agency, reduce costs, and meet or exceed the applicable state and federal laws, regulations, and standards for

information technology security.

(3) Each state agency shall adopt formal procedures for the evaluation of cloud-computing options for existing applications, technology initiatives, or upgrades.

(4) Each state agency shall develop a strategic plan to be updated annually to address its inventory of applications located at the state data center. Each agency shall submit the plan by October 15 of each year to the Office of Policy and Budget in the Executive Office of the Governor and the chairs of the legislative appropriations committees. For each application, the plan must identify and document the readiness, appropriate strategy, and high-level timeline for transition to a cloud-computing service based on the application's quality, cost, and resource requirements. This information must be used to assist the state data center in making adjustments to its service offerings.

(5) Each state agency customer of the state data center shall notify the state data center by May 31 and November 30 annually of any significant changes in its anticipated utilization of state data center services pursuant to requirements established by the state data center.

(6) Unless authorized by the Legislature, the Department of Law Enforcement, as the state's lead Criminal Justice Information Services Systems Agency, may not impose more stringent protection measures than outlined in the federal Criminal Justice Information Services Security Policy relating to the use of cloud-computing services.

Section 12. Section 282.318, Florida Statutes, is amended to read:

282.318 Security of data and information technology.—

(1) This section may be cited as the "Information Technology Security Act."

(2) As used in this section, the term "state agency" has the same meaning as provided in s. 282.0041, except that the term includes the Department of Legal Affairs, the Department of Agriculture and Consumer Services, and the Department of Financial Services.

(3) The department ~~Agency for State Technology~~ is responsible for establishing standards and processes consistent with generally accepted best practices for information technology security, to include cybersecurity, and adopting rules that safeguard an agency's data, information, and information technology resources to ensure availability, confidentiality, and integrity and to mitigate risks. The department ~~agency~~ shall also:

(a) Designate a state chief information security officer who must have experience and expertise in security and risk management for communications and information technology resources.

(b) ~~(a)~~ Develop, and annually update by February 1, a statewide information technology security strategic plan that includes security goals and objectives for the strategic issues of information technology security policy, risk management, training, incident management, and disaster recovery planning.

(c) ~~(b)~~ Develop and publish for use by state agencies an information technology security framework that, at a minimum, includes guidelines and processes for:

1. Establishing asset management procedures to ensure that

an agency's information technology resources are identified and managed consistent with their relative importance to the agency's business objectives.

2. Using a standard risk assessment methodology that includes the identification of an agency's priorities, constraints, risk tolerances, and assumptions necessary to support operational risk decisions.

3. Completing comprehensive risk assessments and information technology security audits, which may be completed by a private sector vendor, and submitting completed assessments and audits to the department ~~Agency for State Technology~~.

4. Identifying protection procedures to manage the protection of an agency's information, data, and information technology resources.

5. Establishing procedures for accessing information and data to ensure the confidentiality, integrity, and availability of such information and data.

6. Detecting threats through proactive monitoring of events, continuous security monitoring, and defined detection processes.

7. Establishing agency computer security incident response teams and describing their responsibilities for responding to information technology security incidents, including breaches of personal information containing confidential or exempt data.

8. Recovering information and data in response to an information technology security incident. The recovery may include recommended improvements to the agency processes, policies, or guidelines.

9. Establishing an information technology security incident

reporting process that includes procedures and tiered reporting timeframes for notifying the department ~~Agency for State Technology~~ and the Department of Law Enforcement of information technology security incidents. The tiered reporting timeframes shall be based upon the level of severity of the information technology security incidents being reported.

10. Incorporating information obtained through detection and response activities into the agency's information technology security incident response plans.

11. Developing agency strategic and operational information technology security plans required pursuant to this section.

12. Establishing the managerial, operational, and technical safeguards for protecting state government data and information technology resources that align with the state agency risk management strategy and that protect the confidentiality, integrity, and availability of information and data.

(d) ~~(c)~~ Assist state agencies in complying with this section.

(e) ~~(d)~~ In collaboration with the Cybercrime Office of the Department of Law Enforcement, annually provide training for state agency information security managers and computer security incident response team members that contains training on information technology security, including cybersecurity, threats, trends, and best practices.

(f) ~~(e)~~ Annually review the strategic and operational information technology security plans of executive branch agencies.

(4) Each state agency head shall, at a minimum:

(a) Designate an information security manager to administer

the information technology security program of the state agency. This designation must be provided annually in writing to the department ~~Agency for State Technology~~ by January 1. A state agency's information security manager, for purposes of these information security duties, shall report directly to the agency head.

(b) In consultation with the department ~~Agency for State Technology~~ and the Cybercrime Office of the Department of Law Enforcement, establish an agency computer security incident response team to respond to an information technology security incident. The agency computer security incident response team shall convene upon notification of an information technology security incident and must comply with all applicable guidelines and processes established pursuant to paragraph (3)(c) ~~paragraph (3)(b)~~.

(c) Submit to the department ~~Agency for State Technology~~ annually by July 31, the state agency's strategic and operational information technology security plans developed pursuant to rules and guidelines established by the department ~~Agency for State Technology~~.

1. The state agency strategic information technology security plan must cover a 3-year period and, at a minimum, define security goals, intermediate objectives, and projected agency costs for the strategic issues of agency information security policy, risk management, security training, security incident response, and disaster recovery. The plan must be based on the statewide information technology security strategic plan created by the department ~~Agency for State Technology~~ and include performance metrics that can be objectively measured to

reflect the status of the state agency's progress in meeting security goals and objectives identified in the agency's strategic information security plan.

2. The state agency operational information technology security plan must include a progress report that objectively measures progress made towards the prior operational information technology security plan and a project plan that includes activities, timelines, and deliverables for security objectives that the state agency will implement during the current fiscal year.

(d) Conduct, and update every 3 years, a comprehensive risk assessment, which may be completed by a private sector vendor, to determine the security threats to the data, information, and information technology resources, including mobile devices and print environments, of the agency. The risk assessment must comply with the risk assessment methodology developed by the department ~~Agency for State Technology~~ and is confidential and exempt from s. 119.07(1), except that such information shall be available to the Auditor General, the Division of State Technology within the department ~~Agency for State Technology~~, the Cybercrime Office of the Department of Law Enforcement, and, for state agencies under the jurisdiction of the Governor, the Chief Inspector General.

(e) Develop, and periodically update, written internal policies and procedures, which include procedures for reporting information technology security incidents and breaches to the Cybercrime Office of the Department of Law Enforcement and the Division of State Technology within the department ~~Agency for State Technology~~. Such policies and procedures must be

consistent with the rules, guidelines, and processes established by the department ~~Agency for State Technology~~ to ensure the security of the data, information, and information technology resources of the agency. The internal policies and procedures that, if disclosed, could facilitate the unauthorized modification, disclosure, or destruction of data or information technology resources are confidential information and exempt from s. 119.07(1), except that such information shall be available to the Auditor General, the Cybercrime Office of the Department of Law Enforcement, the Division of State Technology within the department ~~Agency for State Technology~~, and, for state agencies under the jurisdiction of the Governor, the Chief Inspector General.

(f) Implement managerial, operational, and technical safeguards and risk assessment remediation plans recommended by the department ~~Agency for State Technology~~ to address identified risks to the data, information, and information technology resources of the agency.

(g) Ensure that periodic internal audits and evaluations of the agency's information technology security program for the data, information, and information technology resources of the agency are conducted. The results of such audits and evaluations are confidential information and exempt from s. 119.07(1), except that such information shall be available to the Auditor General, the Cybercrime Office of the Department of Law Enforcement, the Division of State Technology within the department ~~Agency for State Technology~~, and, for agencies under the jurisdiction of the Governor, the Chief Inspector General.

(h) Ensure that the ~~Include appropriate~~ information

technology security and cybersecurity requirements in both the written specifications for the solicitation and service-level agreement of information technology and information technology resources and services meet or exceed the applicable state and federal laws, regulations, and standards for information technology security and cybersecurity. Service-level agreements must identify service provider and state agency responsibilities for privacy and security, protection of government data, personnel background screening, and security deliverables with associated frequencies~~, which are consistent with the rules and guidelines established by the Agency for State Technology in collaboration with the Department of Management Services~~.

(i) Provide information technology security and cybersecurity awareness training to all state agency employees in the first 30 days after commencing employment concerning information technology security risks and the responsibility of employees to comply with policies, standards, guidelines, and operating procedures adopted by the state agency to reduce those risks. The training may be provided in collaboration with the Cybercrime Office of the Department of Law Enforcement.

(j) Develop a process for detecting, reporting, and responding to threats, breaches, or information technology security incidents which is consistent with the security rules, guidelines, and processes established by the Agency for State Technology.

1. All information technology security incidents and breaches must be reported to the Division of State Technology within the department ~~Agency for State Technology~~ and the Cybercrime Office of the Department of Law Enforcement and must

comply with the notification procedures and reporting timeframes established pursuant to paragraph (3)(c) ~~paragraph (3)(b)~~.

2. For information technology security breaches, state agencies shall provide notice in accordance with s. 501.171.

3. Records held by a state agency which identify detection, investigation, or response practices for suspected or confirmed information technology security incidents, including suspected or confirmed breaches, are confidential and exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution, if the disclosure of such records would facilitate unauthorized access to or the unauthorized modification, disclosure, or destruction of:

a. Data or information, whether physical or virtual; or

b. Information technology resources, which includes:

(I) Information relating to the security of the agency's technologies, processes, and practices designed to protect networks, computers, data processing software, and data from attack, damage, or unauthorized access; or

(II) Security information, whether physical or virtual, which relates to the agency's existing or proposed information technology systems.

Such records shall be available to the Auditor General, the Division of State Technology within the department ~~Agency for State Technology~~, the Cybercrime Office of the Department of Law Enforcement, and, for state agencies under the jurisdiction of the Governor, the Chief Inspector General. Such records may be made available to a local government, another state agency, or a federal agency for information technology security purposes or

in furtherance of the state agency's official duties. This exemption applies to such records held by a state agency before, on, or after the effective date of this exemption. This subparagraph is subject to the Open Government Sunset Review Act in accordance with s. 119.15 and shall stand repealed on October 2, 2021, unless reviewed and saved from repeal through reenactment by the Legislature.

(5) The portions of risk assessments, evaluations, external audits, and other reports of a state agency's information technology security program for the data, information, and information technology resources of the state agency which are held by a state agency are confidential and exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution if the disclosure of such portions of records would facilitate unauthorized access to or the unauthorized modification, disclosure, or destruction of:

(a) Data or information, whether physical or virtual; or

(b) Information technology resources, which include:

1. Information relating to the security of the agency's technologies, processes, and practices designed to protect networks, computers, data processing software, and data from attack, damage, or unauthorized access; or

2. Security information, whether physical or virtual, which relates to the agency's existing or proposed information technology systems.

Such portions of records shall be available to the Auditor General, the Cybercrime Office of the Department of Law Enforcement, the Division of State Technology within the

department ~~Agency for State Technology~~, and, for agencies under the jurisdiction of the Governor, the Chief Inspector General. Such portions of records may be made available to a local government, another state agency, or a federal agency for information technology security purposes or in furtherance of the state agency's official duties. For purposes of this subsection, "external audit" means an audit that is conducted by an entity other than the state agency that is the subject of the audit. This exemption applies to such records held by a state agency before, on, or after the effective date of this exemption. This subsection is subject to the Open Government Sunset Review Act in accordance with s. 119.15 and shall stand repealed on October 2, 2021, unless reviewed and saved from repeal through reenactment by the Legislature.

(6) The department ~~Agency for State Technology~~ shall adopt rules relating to information technology security and to administer this section.

Section 13. Subsections (1) and (2) of section 17.0315, Florida Statutes, are amended to read:

17.0315 Financial and cash management system; task force.—

(1) The Chief Financial Officer, as the constitutional officer responsible for settling and approving accounts against the state and keeping all state funds pursuant to s. 4, Art. IV of the State Constitution, is the head of and shall appoint members to a task force established to develop a strategic business plan for a successor financial and cash management system. The task force shall include the state chief information officer ~~executive director of the Agency for State Technology~~ and the director of the Office of Policy and Budget in the

Executive Office of the Governor. Any member of the task force may appoint a designee.

(2) The strategic business plan for a successor financial and cash management system must:

(a) Permit proper disbursement and auditing controls consistent with the respective constitutional duties of the Chief Financial Officer and the Legislature;

(b) Promote transparency in the accounting of public funds;

(c) Provide timely and accurate recording of financial transactions by agencies and their professional staffs;

(d) Support executive reporting and data analysis requirements;

(e) Be capable of interfacing with other systems providing human resource services, procuring goods and services, and providing other enterprise functions;

(f) Be capable of interfacing with the existing legislative appropriations, planning, and budgeting systems;

(g) Be coordinated with the information technology strategy development efforts of the Department of Management Services ~~Agency for State Technology~~;

(h) Be coordinated with the revenue estimating conference process as supported by the Office of Economic and Demographic Research; and

(i) Address other such issues as the Chief Financial Officer identifies.

Section 14. Paragraph (d) of subsection (1) of section 20.055, Florida Statutes, is amended to read:

20.055 Agency inspectors general.—

(1) As used in this section, the term:

(d) "State agency" means each department created pursuant to this chapter and the Executive Office of the Governor, the Department of Military Affairs, the Fish and Wildlife Conservation Commission, the Office of Insurance Regulation of the Financial Services Commission, the Office of Financial Regulation of the Financial Services Commission, the Public Service Commission, the Board of Governors of the State University System, the Florida Housing Finance Corporation, ~~the Agency for State Technology,~~ the Office of Early Learning, and the state courts system.

Section 15. Paragraph (b) of subsection (3) of section 97.0525, Florida Statutes, is amended to read:

97.0525 Online voter registration.—

(3)

(b) The division shall conduct a comprehensive risk assessment of the online voter registration system before making the system publicly available and every 2 years thereafter. The comprehensive risk assessment must comply with the risk assessment methodology developed by the Department of Management Services ~~Agency for State Technology~~ for identifying security risks, determining the magnitude of such risks, and identifying areas that require safeguards.

Section 16. Paragraph (e) of subsection (2) of section 110.205, Florida Statutes, is amended to read:

110.205 Career service; exemptions.—

(2) EXEMPT POSITIONS.—The exempt positions that are not covered by this part include the following:

(e) The state chief information officer ~~executive director of the Agency for State Technology~~. Unless otherwise fixed by

law, the Department of Management Services ~~Agency for State Technology~~ shall set the salary and benefits of this position in accordance with the rules of the Senior Management Service.

Section 17. Subsections (2) and (9) of section 215.322, Florida Statutes, are amended to read:

215.322 Acceptance of credit cards, charge cards, debit cards, or electronic funds transfers by state agencies, units of local government, and the judicial branch.—

(2) A state agency as defined in s. 216.011, or the judicial branch, may accept credit cards, charge cards, debit cards, or electronic funds transfers in payment for goods and services with the prior approval of the Chief Financial Officer. If the Internet or other related electronic methods are to be used as the collection medium, the state chief information officer ~~Agency for State Technology~~ shall review and recommend to the Chief Financial Officer whether to approve the request with regard to the process or procedure to be used.

(9) For payment programs in which credit cards, charge cards, or debit cards are accepted by state agencies, the judicial branch, or units of local government, the Chief Financial Officer, in consultation with the state chief information officer ~~Agency for State Technology~~, may adopt rules to establish uniform security safeguards for cardholder data and to ensure compliance with the Payment Card Industry Data Security Standards.

Section 18. Subsection (2) of section 215.96, Florida Statutes, is amended to read:

215.96 Coordinating council and design and coordination staff.—

(2) The coordinating council shall consist of the Chief Financial Officer; the Commissioner of Agriculture; the Attorney General; the Secretary of Management Services; the state chief information officer ~~executive director of the Agency for State Technology~~; and the Director of Planning and Budgeting, Executive Office of the Governor, or their designees. The Chief Financial Officer, or his or her designee, shall be chair of the council, and the design and coordination staff shall provide administrative and clerical support to the council and the board. The design and coordination staff shall maintain the minutes of each meeting and make such minutes available to any interested person. The Auditor General, the State Courts Administrator, an executive officer of the Florida Association of State Agency Administrative Services Directors, and an executive officer of the Florida Association of State Budget Officers, or their designees, shall serve without voting rights as ex officio members of the council. The chair may call meetings of the council as often as necessary to transact business; however, the council shall meet at least once a year. Action of the council shall be by motion, duly made, seconded and passed by a majority of the council voting in the affirmative for approval of items that are to be recommended for approval to the Financial Management Information Board.

Section 19. Subsection (22) of section 287.057, Florida Statutes, is amended to read:

287.057 Procurement of commodities or contractual services.—

(22) The department, in consultation with the Chief Financial Officer and the state chief information officer ~~Agency~~

~~for State Technology~~, shall maintain a program for online procurement of commodities and contractual services. To enable the state to promote open competition and leverage its buying power, agencies shall participate in the online procurement program, and eligible users may participate in the program. Only vendors prequalified as meeting mandatory requirements and qualifications criteria may participate in online procurement.

(a) The department~~, in consultation with the Agency for State Technology and in compliance with the standards of the agency,~~ may contract for equipment and services necessary to develop and implement online procurement.

(b) The department shall adopt rules to administer the program for online procurement. The rules must include, but not be limited to:

1. Determining the requirements and qualification criteria for prequalifying vendors.

2. Establishing the procedures for conducting online procurement.

3. Establishing the criteria for eligible commodities and contractual services.

4. Establishing the procedures for providing access to online procurement.

5. Determining the criteria warranting any exceptions to participation in the online procurement program.

(c) The department may impose and shall collect all fees for the use of the online procurement systems.

1. The fees may be imposed on an individual transaction basis or as a fixed percentage of the cost savings generated. At a minimum, the fees must be set in an amount sufficient to cover

the projected costs of the services, including administrative and project service costs in accordance with the policies of the department.

2. If the department contracts with a provider for online procurement, the department, pursuant to appropriation, shall compensate the provider from the fees after the department has satisfied all ongoing costs. The provider shall report transaction data to the department each month so that the department may determine the amount due and payable to the department from each vendor.

3. All fees that are due and payable to the state on a transactional basis or as a fixed percentage of the cost savings generated are subject to s. 215.31 and must be remitted within 40 days after receipt of payment for which the fees are due. For fees that are not remitted within 40 days, the vendor shall pay interest at the rate established under s. 55.03(1) on the unpaid balance from the expiration of the 40-day period until the fees are remitted.

4. All fees and surcharges collected under this paragraph shall be deposited in the Operating Trust Fund as provided by law.

Section 20. Section 282.00515, Florida Statutes, is amended to read:

282.00515 Duties of Cabinet agencies.—The Department of Legal Affairs, the Department of Financial Services, and the Department of Agriculture and Consumer Services shall adopt the standards established in s. 282.0051(2), (3), and (7) ~~s. 282.0051(2), (3), and (8)~~ or adopt alternative standards based on best practices and industry standards, and may contract with

the department ~~Agency for State Technology~~ to provide or perform any of the services and functions described in s. 282.0051 for the Department of Legal Affairs, the Department of Financial Services, or the Department of Agriculture and Consumer Services.

Section 21. Subsections (3) and (4) of section 287.0591, Florida Statutes, are amended to read:

287.0591 Information technology.—

(3) The department may execute a state term contract for information technology commodities, consultant services, or staff augmentation contractual services that exceeds the 48-month requirement if the Secretary of Management Services and the state chief information officer ~~executive director of the Agency for State Technology~~ certify to the Executive Office of the Governor that a longer contract term is in the best interest of the state.

(4) If the department issues a competitive solicitation for information technology commodities, consultant services, or staff augmentation contractual services, the Division of State Technology within the department ~~Agency for State Technology~~ shall participate in such solicitations.

Section 22. Paragraph (a) of subsection (3) of section 365.171, Florida Statutes, is amended to read:

365.171 Emergency communications number E911 state plan.—

(3) DEFINITIONS.—As used in this section, the term:

(a) "Office" means the Division of State Technology ~~Program~~ within the Department of Management Services, as designated by the secretary of the department.

Section 23. Paragraph (s) of subsection (3) of section

365.172, Florida Statutes, is amended to read:

365.172 Emergency communications number "E911."—

(3) DEFINITIONS.—Only as used in this section and ss. 365.171, 365.173, and 365.174, the term:

(s) "Office" means the Division of State Technology ~~Program~~ within the Department of Management Services, as designated by the secretary of the department.

Section 24. Paragraph (a) of subsection (1) of section 365.173, Florida Statutes, is amended to read:

365.173 Communications Number E911 System Fund.—

(1) REVENUES.—

(a) Revenues derived from the fee levied on subscribers under s. 365.172(8) must be paid by the board into the State Treasury on or before the 15th day of each month. Such moneys must be accounted for in a special fund to be designated as the Emergency Communications Number E911 System Fund, a fund created in the Division of State Technology ~~Program~~, or other office as designated by the Secretary of Management Services.

Section 25. Subsection (4) of section 445.011, Florida Statutes, is amended to read:

445.011 Workforce information systems.—

(4) CareerSource Florida, Inc., shall coordinate development and implementation of workforce information systems with the state chief information officer ~~executive director of the Agency for State Technology~~ to ensure compatibility with the state's information system strategy and enterprise architecture.

Section 26. Subsection (2) and paragraphs (a) and (b) of subsection (4) of section 445.045, Florida Statutes, are amended to read:

445.045 Development of an Internet-based system for information technology industry promotion and workforce recruitment.—

(2) CareerSource Florida, Inc., shall coordinate with the Department of Management Services ~~Agency for State Technology~~ and the Department of Economic Opportunity to ensure links, as feasible and appropriate, to existing job information websites maintained by the state and state agencies and to ensure that information technology positions offered by the state and state agencies are posted on the information technology website.

(4)(a) CareerSource Florida, Inc., shall coordinate development and maintenance of the website under this section with the state chief information officer ~~executive director of the Agency for State Technology~~ to ensure compatibility with the state's information system strategy and enterprise architecture.

(b) CareerSource Florida, Inc., may enter into an agreement with ~~the Agency for State Technology,~~ the Department of Economic Opportunity~~,~~ or any other public agency with the requisite information technology expertise for the provision of design, operating, or other technological services necessary to develop and maintain the website.

Section 27. Paragraph (b) of subsection (18) of section 668.50, Florida Statutes, is amended to read:

668.50 Uniform Electronic Transaction Act.—

(18) ACCEPTANCE AND DISTRIBUTION OF ELECTRONIC RECORDS BY GOVERNMENTAL AGENCIES.—

(b) To the extent that a governmental agency uses electronic records and electronic signatures under paragraph (a), the Department of Management Services ~~Agency for State~~

~~Technology~~, in consultation with the governmental agency, giving due consideration to security, may specify:

1. The manner and format in which the electronic records must be created, generated, sent, communicated, received, and stored and the systems established for those purposes.

2. If electronic records must be signed by electronic means, the type of electronic signature required, the manner and format in which the electronic signature must be affixed to the electronic record, and the identity of, or criteria that must be met by, any third party used by a person filing a document to facilitate the process.

3. Control processes and procedures as appropriate to ensure adequate preservation, disposition, integrity, security, confidentiality, and auditability of electronic records.

4. Any other required attributes for electronic records which are specified for corresponding nonelectronic records or reasonably necessary under the circumstances.

Section 28. Subsections (4) and (5) of section 943.0415, Florida Statutes, are amended to read:

943.0415 Cybercrime Office.—There is created within the Department of Law Enforcement the Cybercrime Office. The office may:

(4) Provide security awareness training and information to state agency employees concerning cybersecurity, online sexual exploitation of children, and security risks, and the responsibility of employees to comply with policies, standards, guidelines, and operating procedures adopted by the <u>department</u> ~~Agency for State Technology~~.

(5) Consult with the <u>Division of State Technology within</u>

the Department of Management Services ~~Agency for State Technology~~ in the adoption of rules relating to the information technology security provisions in s. 282.318.

Section 29. Florida Cybersecurity Task Force.—

(1) The Florida Cybersecurity Task Force, a task force as defined in s. 20.03(8), Florida Statutes, is created adjunct to the Department of Management Services to review and conduct an assessment of the state's cybersecurity infrastructure, governance, and operations. Except as otherwise provided in this section, the task force shall operate in a manner consistent with s. 20.052, Florida Statutes.

(2) The task force consists of the following members:

(a) The Lieutenant Governor, or his or her designee, who shall serve as chair of the task force.

(b) A representative of the computer crime center of the Department of Law Enforcement, appointed by the executive director of the department.

(c) A representative of the fusion center of the Department of Law Enforcement, appointed by the executive director of the department.

(d) The state chief information officer.

(e) The state chief information security officer.

(f) A representative of the Division of Emergency Management within the Executive Office of the Governor, appointed by the director of the division.

(g) A representative of the Office of the Chief Inspector General in the Executive Office of the Governor, appointed by the Chief Inspector General.

(h) An individual appointed by the President of the Senate.

(i) An individual appointed by the Speaker of the House of Representatives.

(j) Members of the private sector appointed by the Governor.

(3) The task force shall convene by October 1, 2019, and shall meet as necessary, but at least quarterly, at the call of the chair. The Division of State Technology within the Department of Management Services shall provide staffing and administrative support to the task force.

(4) The task force shall:

(a) Recommend methods to secure the state's network systems and data, including standardized plans and procedures to identify developing threats and to prevent unauthorized access and destruction of data.

(b) Identify and recommend remediation, if necessary, of high-risk cybersecurity issues facing state government.

(c) Recommend a process to regularly assess cybersecurity infrastructure and activities of executive branch agencies.

(d) Identify gaps in the state's overall cybersecurity infrastructure, governance, and current operations. Based on any findings of gaps or deficiencies, the task force shall make recommendations for improvement.

(e) Recommend cybersecurity improvements for the state's emergency management and disaster response systems.

(f) Recommend cybersecurity improvements of the state data center.

(g) Review and recommend improvements relating to the state's current operational plans for the response, coordination, and recovery from a cybersecurity attack.

(5) All executive branch departments and agencies shall cooperate fully with requests for information made by the task force.

(6) On or before November 1, 2020, the task force shall submit a final report of its findings and recommendations to the Governor, the President of the Senate, and the Speaker of the House of Representatives.

(7) This section expires January 1, 2021.

Section 30. This act shall take effect July 1, 2019.