The Florida Senate

2024 Florida Statutes (Including 2025C)

Title XIX	**Chapter 282**
PUBLIC BUSINESS	**COMMUNICATIONS AND DATA PROCESSING**

CHAPTER 282
COMMUNICATIONS AND DATA PROCESSING

PART I
INFORMATION TECHNOLOGY MANAGEMENT
(ss. 282.003-282.319)

PART II
ACCESSIBILITY OF INFORMATION AND TECHNOLOGY
(ss. 282.601-282.606)

PART III
COMMUNICATION INFORMATION TECHNOLOGY SERVICES
(ss. 282.701-282.802)

PART I
INFORMATION TECHNOLOGY MANAGEMENT

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

History.—s. 8, ch. 87-137; s. 1, ch. 92-98; s. 93, ch. 92-142; s. 4, ch. 96-390; s. 7, ch. 97-286; s. 45, ch. 99-13; s. 4, ch. 2008-116; s. 5, ch. 2009-80; s. 7, ch. 2019-118.

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

(3) "Breach" has the same meaning as provided in s. 501.171.

(4) "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) "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) "Customer entity" means an entity that obtains services from the Department of Management Services.

(8) "Cybersecurity" means the protection afforded to an automated information system in order to attain the applicable objectives of preserving the confidentiality, integrity, and availability of data, information, and information technology resources.

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

(10) "Data governance" means the practice of organizing, classifying, securing, and implementing policies, procedures, and standards for the effective use of an organization's data.

(11) "Department" means the Department of Management Services.

(12) "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.

(13) "Electronic" means technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.

(14) "Electronic credential" means an electronic representation of the identity of a person, an organization, an application, or a device.

(15) "Enterprise" means state agencies and the Department of Legal Affairs, the Department of Financial Services, and the Department of Agriculture and Consumer Services.

(16) "Enterprise architecture" means a comprehensive operational framework that contemplates the needs and assets of the enterprise to support interoperability.

(17) "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.

(18) "Event" means an observable occurrence in a system or network.

(19) "Incident" means a violation or an imminent threat of violation, whether such violation is accidental or deliberate, of information technology resources, security, policies, or practices. An imminent threat of violation refers to a situation in which a state agency, county, or municipality has a factual basis for believing that a specific incident is about to occur.

(20) "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.

(21) "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.

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

(23) "Interoperability" means the technical ability to share and use data across and throughout the enterprise.

(24) "Open data" means data collected or created by a state agency, the Department of Legal Affairs, the Department of Financial Services, and the Department of Agriculture and Consumer Services, 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 disclosure based on federal or state laws and regulations, including, but not limited to, those related to privacy, confidentiality, security, personal health, business or trade secret information, and exemptions from state public records laws; or data for which a state agency, the Department of Legal Affairs, the Department of Financial Services, or the Department of Agriculture and Consumer Services is statutorily authorized to assess a fee for its distribution.

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

(26) "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.

(27) "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.

(28) "Ransomware incident" means a malicious cybersecurity incident in which a person or an entity introduces software that gains unauthorized access to or encrypts, modifies, or otherwise renders unavailable a state agency's, county's, or municipality's data and thereafter the person or entity demands a ransom to prevent the publication of the data, restore access to the data, or otherwise remediate the impact of the software.

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

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

(31) "Service-level agreement" means a written contract between the Department of Management Services or a provider of data center services and a customer entity which specifies the scope of services provided, the service level, the duration of the agreement, the responsible parties, and the service costs. A service-level agreement is not a rule pursuant to chapter 120.

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

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

(34) "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.

(35) "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.

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

(37) "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.

(38) "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.

History.—ss. 3, 11, ch. 83-92; s. 17, ch. 87-137; ss. 10, 11, ch. 90-160; s. 4, ch. 91-171; s. 10, ch. 91-221; s. 5, ch. 91-429; s. 3, ch. 92-98; s. 95, ch. 92-142; s. 14, ch. 94-226; s. 11, ch. 94-340; s. 9, ch. 97-286; s. 16, ch. 2000-164; s. 51, ch. 2001-61; s. 10, ch. 2001-261; s. 4, ch. 2007-105; s. 5, ch. 2008-116; s. 6, ch. 2009-80; s. 5, ch. 2010-78; s. 9, ch. 2010-148; s. 3, ch. 2011-50; s. 4, ch. 2014-189; s. 9, ch. 2014-221; ss. 58, 61, ch. 2018-10; ss. 78, 81, 82, 115, ch. 2019-116; s. 8, ch. 2019-118; s. 3, ch. 2020-161; s. 2, ch. 2021-234; s. 2, ch. 2022-153; s. 1, ch. 2022-220.

Note.—Former s. 282.303.

282.0051 Department of Management Services; Florida Digital Service; powers, duties, and functions.—

(1) The Florida Digital Service has been created within the department to propose innovative solutions that securely modernize state government, including technology and information services, to achieve value through digital transformation and interoperability, and to fully support the cloud-first policy as specified in s. 282.206. The department, through the Florida Digital Service, shall have the following powers, duties, and functions:

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

(b) Develop an enterprise architecture that:

1. Acknowledges the unique needs of the entities within the enterprise in the development and publication of standards and terminologies to facilitate digital interoperability;

2. Supports the cloud-first policy as specified in s. 282.206; and

3. Addresses how information technology infrastructure may be modernized to achieve cloud-first objectives.

(c) Establish project management and oversight standards with which state agencies must comply when implementing information technology projects. The department, acting through the Florida Digital Service, 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:

1. 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.

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

3. 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.

4. Content, format, and frequency of project updates.

5. Technical standards to ensure an information technology project complies with the enterprise architecture.

(d) 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, acting through the Florida Digital Service, 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 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.

(e) Identify opportunities for standardization and consolidation of information technology services that support interoperability and the cloud-first policy, as specified in s. 282.206, and 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, acting through the Florida Digital Service, shall biennially on January 1 of each even-numbered year 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.

(f) 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, or improve government services.

(g) 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.

(h) Upon request, assist state agencies in the development of information technology-related legislative budget requests.

(i) Conduct annual assessments of state agencies to determine compliance with all information technology standards and guidelines developed and published by the department 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.

(j) Conduct a market analysis not less frequently than every 3 years beginning in 2021 to determine whether the information technology resources within the enterprise are utilized in the most cost-effective and cost-efficient manner, while recognizing that the replacement of certain legacy information technology systems within the enterprise may be cost prohibitive or cost inefficient due to the remaining useful life of those resources; whether the enterprise is complying with the cloud-first policy specified in s. 282.206; and whether the enterprise is utilizing best practices with respect to information technology, information services, and the acquisition of emerging technologies and information services. Each market analysis shall be used to prepare a strategic plan for continued and future information technology and information services for the enterprise, including, but not limited to, proposed acquisition of new services or technologies and approaches to the implementation of any new services or technologies. Copies of each market analysis and accompanying strategic plan must be submitted to the Executive Office of the Governor, the President of the Senate, and the Speaker of the House of Representatives not later than December 31 of each year that a market analysis is conducted.

(k) 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.

(l) 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.

(m)1. 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 has a total project cost of $20 million or more. Such information technology projects must also comply with the applicable information technology architecture, project management and oversight, and reporting standards established by the department, acting through the Florida Digital Service.

2. When performing the project oversight function specified in subparagraph 1., 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, acting through the Florida Digital Service, 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.

(n) 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.

(o) If adherence to standards or policies adopted by or established pursuant to this section causes conflict with federal regulations or requirements imposed on an entity within the enterprise and results in adverse action against an entity or federal funding, work with the entity to provide alternative standards, policies, or requirements that do not conflict with the federal regulation or requirement. The department, acting through the Florida Digital Service, shall annually report such alternative standards to the Executive Office of the Governor, the President of the Senate, and the Speaker of the House of Representatives.

(p)1. 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:

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

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

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

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

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

f. At a minimum, a requirement that any contract for information technology commodities or services meet the National Institute of Standards and Technology Cybersecurity Framework.

g. For an information technology project wherein project oversight is required pursuant to paragraph (d) or paragraph (m), a requirement that independent verification and validation be employed throughout the project life cycle with the primary objective of independent verification and validation being to provide an objective assessment of products and processes throughout the project life cycle. An entity providing independent verification and validation may not have technical, managerial, or financial interest in the project and may not have responsibility for, or participate in, any other aspect of the project.

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

3. Answer vendor questions on information technology-related state term contract solicitations.

4. Ensure that the information technology policy established pursuant to subparagraph 1. is included in all solicitations and contracts that are administratively executed by the department.

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

(r) Recommend open data technical standards and terminologies for use by the enterprise.

(s) Ensure that enterprise information technology solutions are capable of utilizing an electronic credential and comply with the enterprise architecture standards.

(2)(a) The Secretary of Management Services shall designate a state chief information officer, who shall administer the Florida Digital Service. The state chief information officer, prior to appointment, must have at least 5 years of experience in the development of information system strategic planning and development or information technology policy, and, preferably, have leadership-level experience in the design, development, and deployment of interoperable software and data solutions.

(b) The state chief information officer, in consultation with the Secretary of Management Services, shall designate a state chief data officer. The chief data officer must be a proven and effective administrator who must have significant and substantive experience in data management, data governance, interoperability, and security.

(3) The department, acting through the Florida Digital Service and from funds appropriated to the Florida Digital Service, shall:

(a) Create, not later than December 1, 2022, and maintain a comprehensive indexed data catalog in collaboration with the enterprise that lists the data elements housed within the enterprise and the legacy system or application in which these data elements are located. The data catalog must, at a minimum, specifically identify all data that is restricted from public disclosure based on federal or state laws and regulations and require that all such information be protected in accordance with s. 282.318.

(b) Develop and publish, not later than December 1, 2022, in collaboration with the enterprise, a data dictionary for each agency that reflects the nomenclature in the comprehensive indexed data catalog.

(c) Adopt, by rule, standards that support the creation and deployment of an application programming interface to facilitate integration throughout the enterprise.

(d) Adopt, by rule, standards necessary to facilitate a secure ecosystem of data interoperability that is compliant with the enterprise architecture.

(e) Adopt, by rule, standards that facilitate the deployment of applications or solutions to the existing enterprise system in a controlled and phased approach.

(f) After submission of documented use cases developed in conjunction with the affected agencies, assist the affected agencies with the deployment, contingent upon a specific appropriation therefor, of new interoperable applications and solutions:

1. For the Department of Health, the Agency for Health Care Administration, the Agency for Persons with Disabilities, the Department of Education, the Department of Elderly Affairs, and the Department of Children and Families.

2. To support military members, veterans, and their families.

(4) For information technology projects that have a total project cost of $10 million or more:

(a) State agencies must provide the Florida Digital Service with written notice of any planned procurement of an information technology project.

(b) The Florida Digital Service must participate in the development of specifications and recommend modifications to any planned procurement of an information technology project by state agencies so that the procurement complies with the enterprise architecture.

(c) The Florida Digital Service must participate in post-award contract monitoring.

(5) The department, acting through the Florida Digital Service, may not retrieve or disclose any data without a shared-data agreement in place between the department and the enterprise entity that has primary custodial responsibility of, or data-sharing responsibility for, that data.

(6) The department, acting through the Florida Digital Service, shall adopt rules to administer this section.

History.—s. 10, ch. 2014-221; s. 3, ch. 2016-138; ss. 59, 61, ch. 2018-10; ss. 79, 81, 82, 115, ch. 2019-116; s. 9, ch. 2019-118; s. 4, ch. 2020-161; s. 1, ch. 2021-227; s. 3, ch. 2021-234; s. 3, ch. 2022-153.

282.00515 Duties of Cabinet agencies.—

(1) 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(1)(b), (c), and (r) and (3)(e) or adopt alternative standards based on best practices and industry standards that allow for open data interoperability.

(2) If the Department of Legal Affairs, the Department of Financial Services, or the Department of Agriculture and Consumer Services adopts alternative standards in lieu of the enterprise architecture standards adopted pursuant to s. 282.0051, such department must notify the Governor, the President of the Senate, and the Speaker of the House of Representatives in writing of the adoption of the alternative standards and provide a justification for adoption of the alternative standards and explain how the agency will achieve open data interoperability.

(3) The Department of Legal Affairs, the Department of Financial Services, and the Department of Agriculture and Consumer Services may contract with the department to provide or perform any of the services and functions described in s. 282.0051.

(4)(a) Nothing in this section or in s. 282.0051 requires the Department of Legal Affairs, the Department of Financial Services, or the Department of Agriculture and Consumer Services to integrate with information technology outside its own department or with the Florida Digital Service.

(b) The department, acting through the Florida Digital Service, may not retrieve or disclose any data without a shared-data agreement in place between the department and the Department of Legal Affairs, the Department of Financial Services, or the Department of Agriculture and Consumer Services.

History.—s. 11, ch. 2014-221; s. 20, ch. 2019-118; s. 5, ch. 2020-161; s. 6, ch. 2022-153.

282.201 State data center.— The state data center is established within the department. 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 who has experience in leading data center facilities and has expertise in cloud-computing management.

(1) 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 business continuity and disaster recovery plans, and annually 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 by agency application, 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 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 consolidation, 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 cybersecurity.

(h) Assist customer entities in transitioning from state data center services to the Northwest Regional Data Center or other third-party cloud-computing services procured by a customer entity or by the Northwest Regional Data Center on behalf of a customer entity.

[1](2) USE OF THE STATE DATA CENTER.—

(a) The following are exempt from the use of the state data center: 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.

(b) The Division of Emergency Management is exempt from the use of the state data center. This paragraph expires July 1, 2025.

(3) AGENCY LIMITATIONS.—Unless exempt from the use of the state data center pursuant to this section or authorized by the Legislature, a state agency may not:

(a) 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

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

(4) DEPARTMENT RESPONSIBILITIES.—The department shall provide operational management and oversight of the state data center, 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. The department may recommend other payment mechanisms to the Executive Office of the Governor, the President of the Senate, and the Speaker of the House of Representatives. Such mechanisms may be implemented only if specifically authorized by the Legislature.

(c) Developing and implementing appropriate operating guidelines and procedures necessary for the state data center to perform its duties pursuant to subsection (1). 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 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 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 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 and the Florida Digital Service, developing and implementing a process for detecting, reporting, and responding to cybersecurity 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.

(5) NORTHWEST REGIONAL DATA CENTER CONTRACT.—In order for the department to carry out its duties and responsibilities relating to the state data center, the secretary of the department shall contract by July 1, 2022, with the Northwest Regional Data Center pursuant to s. 287.057(11). The contract shall provide that the Northwest Regional Data Center will manage the operations of the state data center and provide data center services to state agencies.

(a) The department shall provide contract oversight, including, but not limited to, reviewing invoices provided by the Northwest Regional Data Center for services provided to state agency customers.

(b) The department shall approve or request updates to invoices within 10 business days after receipt. If the department does not respond to the Northwest Regional Data Center, the invoice will be approved by default. The Northwest Regional Data Center must submit approved invoices directly to state agency customers.

History.—s. 8, ch. 2008-116; s. 24, ch. 2009-21; s. 8, ch. 2009-80; s. 44, ch. 2010-5; s. 2, ch. 2010-148; s. 5, ch. 2011-50; s. 33, ch. 2012-96; s. 2, ch. 2012-134; s. 1, ch. 2012-142; s. 37, ch. 2013-15; ss. 47, 48, ch. 2013-41; s. 50, ch. 2014-19; ss. 13, 14, ch. 2014-221; ss. 60, 61, ch. 2018-10; ss. 80, 81, 82, 115, ch. 2019-116; s. 10, ch. 2019-118; s. 47, ch. 2020-2; s. 4, ch. 2021-234; s. 4, ch. 2022-153; s. 85, ch. 2024-228.

[1]**Note.**—Section 85, ch. 2024-228, amended subsection (2) "in order to implement Specific Appropriation 2693A of the 2024-2025 General Appropriations [A]ct."

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 cybersecurity.

(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.

History.—s. 11, ch. 2019-118; s. 5, ch. 2021-234.

282.318 Cybersecurity.—

(1) This section may be cited as the "State Cybersecurity 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, acting through the Florida Digital Service, is the lead entity responsible for establishing standards and processes for assessing state agency cybersecurity risks and determining appropriate security measures. Such standards and processes must be consistent with generally accepted technology best practices, including the National Institute for Standards and Technology Cybersecurity Framework, for cybersecurity. The department, acting through the Florida Digital Service, shall adopt rules that mitigate risks; safeguard state agency digital assets, data, information, and information technology resources to ensure availability, confidentiality, and integrity; and support a security governance framework. The department, acting through the Florida Digital Service, shall also:

(a) Designate an employee of the Florida Digital Service as the state chief information security officer. The state chief information security officer must have experience and expertise in security and risk management for communications and information technology resources. The state chief information security officer is responsible for the development, operation, and oversight of cybersecurity for state technology systems. The state chief information security officer shall be notified of all confirmed or suspected incidents or threats of state agency information technology resources and must report such incidents or threats to the state chief information officer and the Governor.

(b) Develop, and annually update by February 1, a statewide cybersecurity strategic plan that includes security goals and objectives for cybersecurity, including the identification and mitigation of risk, proactive protections against threats, tactical risk detection, threat reporting, and response and recovery protocols for a cyber incident.

(c) Develop and publish for use by state agencies a cybersecurity governance 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 cybersecurity audits, which may be completed by a private sector vendor, and submitting completed assessments and audits to the department.

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 cybersecurity incident response teams and describing their responsibilities for responding to cybersecurity incidents, including breaches of personal information containing confidential or exempt data.

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

9. Establishing a cybersecurity incident reporting process that includes procedures for notifying the department and the Department of Law Enforcement of cybersecurity incidents.

a. The level of severity of the cybersecurity incident is defined by the National Cyber Incident Response Plan of the United States Department of Homeland Security as follows:

(I) Level 5 is an emergency-level incident within the specified jurisdiction that poses an imminent threat to the provision of wide-scale critical infrastructure services; national, state, or local government security; or the lives of the country's, state's, or local government's residents.

(II) Level 4 is a severe-level incident that is likely to result in a significant impact in the affected jurisdiction to public health or safety; national, state, or local security; economic security; or civil liberties.

(III) Level 3 is a high-level incident that is likely to result in a demonstrable impact in the affected jurisdiction to public health or safety; national, state, or local security; economic security; civil liberties; or public confidence.

(IV) Level 2 is a medium-level incident that may impact public health or safety; national, state, or local security; economic security; civil liberties; or public confidence.

(V) Level 1 is a low-level incident that is unlikely to impact public health or safety; national, state, or local security; economic security; civil liberties; or public confidence.

b. The cybersecurity incident reporting process must specify the information that must be reported by a state agency following a cybersecurity incident or ransomware incident, which, at a minimum, must include the following:

(I) A summary of the facts surrounding the cybersecurity incident or ransomware incident.

(II) The date on which the state agency most recently backed up its data; the physical location of the backup, if the backup was affected; and if the backup was created using cloud computing.

(III) The types of data compromised by the cybersecurity incident or ransomware incident.

(IV) The estimated fiscal impact of the cybersecurity incident or ransomware incident.

(V) In the case of a ransomware incident, the details of the ransom demanded.

c.(I) A state agency shall report all ransomware incidents and any cybersecurity incident determined by the state agency to be of severity level 3, 4, or 5 to the Cybersecurity Operations Center and the Cybercrime Office of the Department of Law Enforcement as soon as possible but no later than 48 hours after discovery of the cybersecurity incident and no later than 12 hours after discovery of the ransomware incident. The report must contain the information required in sub-subparagraph b.

(II) The Cybersecurity Operations Center shall notify the President of the Senate and the Speaker of the House of Representatives of any severity level 3, 4, or 5 incident as soon as possible but no later than 12 hours after receiving a state agency's incident report. The notification must include a high-level description of the incident and the likely effects.

d. A state agency shall report a cybersecurity incident determined by the state agency to be of severity level 1 or 2 to the Cybersecurity Operations Center and the Cybercrime Office of the Department of Law Enforcement as soon as possible. The report must contain the information required in sub-subparagraph b.

e. The Cybersecurity Operations Center shall provide a consolidated incident report on a quarterly basis to the President of the Senate, the Speaker of the House of Representatives, and the Florida Cybersecurity Advisory Council. The report provided to the Florida Cybersecurity Advisory Council may not contain the name of any agency, network

information, or system identifying information but must contain sufficient relevant information to allow the Florida Cybersecurity Advisory Council to fulfill its responsibilities as required in s. 282.319(9).

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

11. Developing agency strategic and operational cybersecurity 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.

13. Establishing procedures for procuring information technology commodities and services that require the commodity or service to meet the National Institute of Standards and Technology Cybersecurity Framework.

14. Submitting after-action reports following a cybersecurity incident or ransomware incident. Such guidelines and processes for submitting after-action reports must be developed and published by December 1, 2022.

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

(e) 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 cybersecurity, including cybersecurity threats, trends, and best practices.

(f) Annually review the strategic and operational cybersecurity plans of state agencies.

(g) Annually provide cybersecurity training to all state agency technology professionals and employees with access to highly sensitive information which develops, assesses, and documents competencies by role and skill level. The cybersecurity training curriculum must include training on the identification of each cybersecurity incident severity level referenced in sub-subparagraph (c)9.a. The training may be provided in collaboration with the Cybercrime Office of the Department of Law Enforcement, a private sector entity, or an institution of the State University System.

(h) Operate and maintain a Cybersecurity Operations Center led by the state chief information security officer, which must be primarily virtual and staffed with tactical detection and incident response personnel. The Cybersecurity Operations Center shall serve as a clearinghouse for threat information and coordinate with the Department of Law Enforcement to support state agencies and their response to any confirmed or suspected cybersecurity incident.

(i) Lead an Emergency Support Function, ESF CYBER, under the state comprehensive emergency management plan as described in s. 252.35.

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

(a) Designate an information security manager to administer the cybersecurity program of the state agency. This designation must be provided annually in writing to the department 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, through the Florida Digital Service, and the Cybercrime Office of the Department of Law Enforcement, establish an agency cybersecurity response team to respond to a cybersecurity incident. The agency cybersecurity response team shall convene upon notification of a cybersecurity incident and must immediately report all confirmed or suspected incidents to the state chief information security officer, or his or her designee, and comply with all applicable guidelines and processes established pursuant to paragraph (3)(c).

(c) Submit to the department annually by July 31, the state agency's strategic and operational cybersecurity plans developed pursuant to rules and guidelines established by the department, through the Florida Digital Service.

1. The state agency strategic cybersecurity 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 cybersecurity strategic plan created by the department 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 cybersecurity plan must include a progress report that objectively measures progress made towards the prior operational cybersecurity 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 and is confidential and exempt from s. 119.07(1), except that such information shall be available to the Auditor General, the Florida Digital Service within the department, the Cybercrime Office of the Department of Law Enforcement, and, for state agencies under the jurisdiction of the Governor, the Chief Inspector General. If a private sector vendor is used to complete a comprehensive risk assessment, it must attest to the validity of the risk assessment findings.

(e) Develop, and periodically update, written internal policies and procedures, which include procedures for reporting cybersecurity incidents and breaches to the Cybercrime Office of the Department of Law Enforcement and the Florida Digital Service within the department. Such policies and procedures must be consistent with the rules, guidelines, and processes established by the department 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 Florida Digital Service within the department, 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 to address identified risks to the data, information, and information technology resources of the agency. The department, through the Florida Digital Service, shall track implementation by state agencies upon development of such remediation plans in coordination with agency inspectors general.

(g) Ensure that periodic internal audits and evaluations of the agency's cybersecurity 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 Florida Digital Service within the department, and, for agencies under the jurisdiction of the Governor, the Chief Inspector General.

(h) Ensure that the cybersecurity requirements in the written specifications for the solicitation, contracts, 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 cybersecurity, including the National Institute of Standards and Technology Cybersecurity Framework. 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.

(i) Provide cybersecurity awareness training to all state agency employees within 30 days after commencing employment, and annually thereafter, concerning cybersecurity 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, a private sector entity, or an institution of the State University System.

(j) Develop a process for detecting, reporting, and responding to threats, breaches, or cybersecurity incidents which is consistent with the security rules, guidelines, and processes established by the department through the Florida Digital Service.

1. All cybersecurity incidents and ransomware incidents must be reported by state agencies. Such reports must comply with the notification procedures and reporting timeframes established pursuant to paragraph (3)(c).

2. For cybersecurity breaches, state agencies shall provide notice in accordance with s. 501.171.

(k) Submit to the Florida Digital Service, within 1 week after the remediation of a cybersecurity incident or ransomware incident, an after-action report that summarizes the incident, the incident's resolution, and any insights gained as a result of the incident.

(5) The portions of risk assessments, evaluations, external audits, and other reports of a state agency's cybersecurity 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.

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.

(6) Those portions of a public meeting as specified in s. 286.011 which would reveal records which are confidential and exempt under subsection (5) are exempt from s. 286.011 and s. 24(b), Art. I of the State Constitution. No exempt portion of an exempt meeting may be off the record. All exempt portions of such meeting shall be recorded and transcribed. Such recordings and transcripts are confidential and exempt from disclosure under s. 119.07(1) and s. 24(a), Art. I of the State Constitution unless a court of competent jurisdiction, after an in camera review, determines that the meeting was not restricted to the discussion of data and information made confidential and exempt by this section. In the event of such a judicial determination, only that portion of the recording and transcript which reveals nonexempt data and information may be disclosed to a third party.

(7) The portions of records made confidential and exempt in subsections (5) and (6) shall be available to the Auditor General, the Cybercrime Office of the Department of Law Enforcement, the Florida Digital Service within the department, 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 cybersecurity purposes or in furtherance of the state agency's official duties.

(8) The exemptions contained in subsections (5) and (6) apply to records held by a state agency before, on, or after the effective date of this exemption.

(9) Subsections (5) and (6) are subject to the Open Government Sunset Review Act in accordance with s. 119.15 and shall stand repealed on October 2, 2025, unless reviewed and saved from repeal through reenactment by the Legislature.

(10) The department shall adopt rules relating to cybersecurity and to administer this section.

History.—ss. 1, 2, 3, ch. 84-236; s. 28, ch. 87-137; s. 1, ch. 89-14; s. 7, ch. 90-160; s. 13, ch. 91-171; s. 234, ch. 92-279; s. 55, ch. 92-326; s. 22, ch. 94-340; s. 863, ch. 95-148; s. 131, ch. 96-406; s. 15, ch. 97-286; s. 25, ch. 2000-164; s. 26, ch. 2001-261; s. 18, ch. 2006-26; s. 10, ch. 2007-105; s. 12, ch. 2009-80; s. 46, ch. 2010-5; s. 9, ch. 2011-50; s. 5, ch. 2014-189; s. 16, ch. 2014-221; s. 1, ch. 2016-114; s. 2, ch. 2016-138; s. 12, ch. 2019-118; s. 48, ch. 2020-2; s. 1, ch. 2020-25; s. 6, ch. 2020-161; s. 6, ch. 2021-234; s. 13, ch. 2022-4; s. 2, ch. 2022-220; s. 3, ch. 2022-221.

282.3185 Local government cybersecurity.—

(1) SHORT TITLE.—This section may be cited as the "Local Government Cybersecurity Act."

(2) DEFINITION.—As used in this section, the term "local government" means any county or municipality.

(3) CYBERSECURITY TRAINING.—

(a) The Florida Digital Service shall:

1. Develop a basic cybersecurity training curriculum for local government employees. All local government employees with access to the local government's network must complete the basic cybersecurity training within 30 days after commencing employment and annually thereafter.

2. Develop an advanced cybersecurity training curriculum for local governments which is consistent with the cybersecurity training required under s. 282.318(3)(g). All local government technology professionals and employees with access to highly sensitive information must complete the advanced cybersecurity training within 30 days after commencing employment and annually thereafter.

(b) The Florida Digital Service may provide the cybersecurity training required by this subsection in collaboration with the Cybercrime Office of the Department of Law Enforcement, a private sector entity, or an institution of the State University System.

(4) CYBERSECURITY STANDARDS.—

(a) Each local government shall adopt cybersecurity standards that safeguard its data, information technology, and information technology resources to ensure availability, confidentiality, and integrity. The cybersecurity standards must be consistent with generally accepted best practices for cybersecurity, including the National Institute of Standards and Technology Cybersecurity Framework.

(b) Each county with a population of 75,000 or more must adopt the cybersecurity standards required by this subsection by January 1, 2024. Each county with a population of less than 75,000 must adopt the cybersecurity standards required by this subsection by January 1, 2025.

(c) Each municipality with a population of 25,000 or more must adopt the cybersecurity standards required by this subsection by January 1, 2024. Each municipality with a population of less than 25,000 must adopt the cybersecurity standards required by this subsection by January 1, 2025.

(d) Each local government shall notify the Florida Digital Service of its compliance with this subsection as soon as possible.

(5) INCIDENT NOTIFICATION.—

(a) A local government shall provide notification of a cybersecurity incident or ransomware incident to the Cybersecurity Operations Center, Cybercrime Office of the Department of Law Enforcement, and sheriff who has jurisdiction over the local government in accordance with paragraph (b). The notification must include, at a minimum, the following information:

1. A summary of the facts surrounding the cybersecurity incident or ransomware incident.
2. The date on which the local government most recently backed up its data; the physical location of the backup, if the backup was affected; and if the backup was created using cloud computing.
3. The types of data compromised by the cybersecurity incident or ransomware incident.
4. The estimated fiscal impact of the cybersecurity incident or ransomware incident.
5. In the case of a ransomware incident, the details of the ransom demanded.
6. A statement requesting or declining assistance from the Cybersecurity Operations Center, the Cybercrime Office of the Department of Law Enforcement, or the sheriff who has jurisdiction over the local government.

(b)1. A local government shall report all ransomware incidents and any cybersecurity incident determined by the local government to be of severity level 3, 4, or 5 as provided in s. 282.318(3)(c) to the Cybersecurity Operations Center, the Cybercrime Office of the Department of Law Enforcement, and the sheriff who has jurisdiction over the local government as soon as possible but no later than 48 hours after discovery of the cybersecurity incident and no later than 12 hours after discovery of the ransomware incident. The report must contain the information required in paragraph (a).

2. The Cybersecurity Operations Center shall notify the President of the Senate and the Speaker of the House of Representatives of any severity level 3, 4, or 5 incident as soon as possible but no later than 12 hours after receiving a local government's incident report. The notification must include a high-level description of the incident and the likely effects.

(c) A local government may report a cybersecurity incident determined by the local government to be of severity level 1 or 2 as provided in s. 282.318(3)(c) to the Cybersecurity Operations Center, the Cybercrime Office of the Department of Law Enforcement, and the sheriff who has jurisdiction over the local government. The report shall contain the information required in paragraph (a).

(d) The Cybersecurity Operations Center shall provide a consolidated incident report on a quarterly basis to the President of the Senate, the Speaker of the House of Representatives, and the Florida Cybersecurity Advisory Council. The report provided to the Florida Cybersecurity Advisory Council may not contain the name of any local government, network information, or system identifying information but must contain sufficient relevant information to allow the Florida Cybersecurity Advisory Council to fulfill its responsibilities as required in s. 282.319(9).

(6) AFTER-ACTION REPORT.—A local government must submit to the Florida Digital Service, within 1 week after the remediation of a cybersecurity incident or ransomware incident, an after-action report that summarizes the incident, the incident's resolution, and any insights gained as a result of the incident. By December 1, 2022, the Florida Digital Service shall establish guidelines and processes for submitting an after-action report.

History.—s. 3, ch. 2022-220.

282.3186 Ransomware incident compliance.— A state agency as defined in s. 282.318(2), a county, or a municipality experiencing a ransomware incident may not pay or otherwise comply with a ransom demand.

History.—s. 4, ch. 2022-220.

282.319 Florida Cybersecurity Advisory Council.—

(1) The Florida Cybersecurity Advisory Council, an advisory council as defined in s. 20.03(7), is created within the department. Except as otherwise provided in this section, the advisory council shall operate in a manner consistent with s. 20.052.

(2) The purpose of the council is to:

(a) Assist state agencies in protecting their information technology resources from cybersecurity threats and incidents.

(b) Advise counties and municipalities on cybersecurity, including cybersecurity threats, trends, and best practices.

(3) The council shall assist the Florida Digital Service in implementing best cybersecurity practices, taking into consideration the final recommendations of the Florida Cybersecurity Task Force created under chapter 2019-118, Laws of Florida.

(4) The council shall be comprised of the following members:

(a) The Lieutenant Governor or his or her designee.

(b) The state chief information officer.

(c) The state chief information security officer.

(d) The director of the Division of Emergency Management or his or her designee.

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

(f) A representative of the Florida Fusion Center of the Department of Law Enforcement, appointed by the executive director of the Department of Law Enforcement.

(g) The Chief Inspector General.

(h) A representative from the Public Service Commission.

(i) Up to two representatives from institutions of higher education located in this state, appointed by the Governor.

(j) Three representatives from critical infrastructure sectors, one of whom must be from a water treatment facility, appointed by the Governor.

(k) Four representatives of the private sector with senior level experience in cybersecurity or software engineering from within the finance, energy, health care, and transportation sectors, appointed by the Governor.

(l) Two representatives with expertise on emerging technology, with one appointed by the President of the Senate and one appointed by the Speaker of the House of Representatives.

(5) Members shall serve for a term of 4 years; however, for the purpose of providing staggered terms, the initial appointments of members made by the Governor shall be for a term of 2 years. A vacancy shall be filled for the remainder of the unexpired term in the same manner as the initial appointment. All members of the council are eligible for reappointment.

(6) The Secretary of Management Services, or his or her designee, shall serve as the ex officio, nonvoting executive director of the council.

(7) Members of the council shall serve without compensation but are entitled to receive reimbursement for per diem and travel expenses pursuant to s. 112.061.

(8) Members of the council shall maintain the confidential or exempt status of information received in the performance of their duties and responsibilities as members of the council. In accordance with s. 112.313, a current or former member of the council may not disclose or use information not available to the general public and gained by reason of their official position, except for information relating exclusively to governmental practices, for their personal gain or benefit or for the personal gain or benefit of any other person or business entity. Members shall sign an agreement acknowledging the provisions of this subsection.

(9) The council shall meet at least quarterly to:

(a) Review existing state agency cybersecurity policies.

(b) Assess ongoing risks to state agency information technology.

(c) Recommend a reporting and information sharing system to notify state agencies of new risks.

(d) Recommend data breach simulation exercises.

(e) Assist the Florida Digital Service in developing cybersecurity best practice recommendations for state agencies that include recommendations regarding:

1. Continuous risk monitoring.
2. Password management.
3. Protecting data in legacy and new systems.

(f) Examine inconsistencies between state and federal law regarding cybersecurity.

(g) Review information relating to cybersecurity incidents and ransomware incidents to determine commonalities and develop best practice recommendations for state agencies, counties, and municipalities.

(h) Recommend any additional information that a county or municipality should report to the Florida Digital Service as part of its cybersecurity incident or ransomware incident notification pursuant to s. 282.3185.

(10) The council shall work with the National Institute of Standards and Technology and other federal agencies, private sector businesses, and private cybersecurity experts:

(a) For critical infrastructure not covered by federal law, to identify which local infrastructure sectors are at the greatest risk of cyber attacks and need the most enhanced cybersecurity measures.

(b) To use federal guidance to identify categories of critical infrastructure as critical cyber infrastructure if cyber damage or unauthorized cyber access to the infrastructure could reasonably result in catastrophic consequences.

(11) Each June 30, the council shall submit to the President of the Senate and the Speaker of the House of Representatives any legislative recommendations considered necessary by the council to address cybersecurity.

(12) Each December 1, the council shall submit to the Governor, the President of the Senate, and the Speaker of the House of Representatives a comprehensive report that includes data, trends, analysis, findings, and recommendations for state and local action regarding ransomware incidents. At a minimum, the report must include:

(a) Descriptive statistics including the amount of ransom requested, the duration of the ransomware incident, and the overall monetary cost to taxpayers of the ransomware incident.

(b) A detailed statistical analysis of the circumstances that led to the ransomware incident which does not include the name of the state agency, county, or municipality; network information; or system identifying information.

(c) A detailed statistical analysis of the level of cybersecurity employee training and frequency of data backup for the state agency, county, or municipality that reported the ransomware incident.

(d) Specific issues identified with current policies, procedures, rules, or statutes and recommendations to address such issues.

(e) Any other recommendations to prevent ransomware incidents.

(13) For purposes of this section, the term "state agency" has the same meaning as provided in s. 282.318(2).

History.—s. 7, ch. 2021-234; s. 14, ch. 2022-4; s. 5, ch. 2022-220; s. 57, ch. 2023-8.

PART II
ACCESSIBILITY OF INFORMATION AND TECHNOLOGY

282.601 Accessibility of electronic information and information technology.—

(1) In order to improve the accessibility of electronic information and information technology and increase the successful education, employment, access to governmental information and services, and involvement in community life, the executive, legislative, and judicial branches of state government shall, when developing, competitively procuring, maintaining, or using electronic information or information technology acquired on or after July 1, 2006, ensure that state employees with disabilities have access to and are provided with information and data comparable to the access and use by state employees who are not individuals with disabilities, unless an undue burden would be imposed on the agency.

(2) Individuals with disabilities who are members of the public seeking information or services from state agencies that are subject to this part shall be provided with access to and use of information and data comparable to that provided to the public who are not individuals with disabilities, unless an undue burden would be imposed on the agency.

History.—s. 73, ch. 2006-227.

282.602 Definitions.— As used in this part, the term:

(1) "Accessible electronic information and information technology" means electronic information and information technology that conforms to the standards for accessible electronic information and information technology as set forth by s. 508 of the Rehabilitation Act of 1973, as amended, and 29 U.S.C. s. 794(d), including the regulations set forth under 36 C.F.R. part 1194.

(2) "Alternate methods" means a different means of providing information to people with disabilities, including product documentation. The term includes, but is not limited to, voice, facsimile, relay service, TTY, Internet posting, captioning, text-to-speech synthesis, and audio description.

(3) "Electronic information and information technology" includes information technology and any equipment or interconnected system or subsystem of equipment that is used in creating, converting, or duplicating data or information. The term includes, but is not limited to, telecommunications products such as telephones, information kiosks and transaction machines, Internet websites, multimedia systems, and office equipment such as copiers and facsimile machines. The term does not include any equipment that contains embedded information technology that is an integral part of the product if the principal function of the technology is not the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.

(4) "Information technology" means any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. The term includes computers, ancillary equipment, software, firmware and similar procedures, services, and support services, and related resources.

(5) "Undue burden" means significant difficulty or expense. In determining whether an action would result in an undue burden, a state agency shall consider all agency resources that are available to the program or component for which the product is being developed, procured, maintained, or used.

(6) "State agency" means any agency of the executive, legislative, or judicial branch of state government.

History.—s. 73, ch. 2006-227.

282.603 Access to electronic and information technology for persons with disabilities; undue burden; limitations.—

(1) Each state agency shall develop, procure, maintain, and use accessible electronic information and information technology acquired on or after July 1, 2006, that conforms to the applicable provisions set forth by s. 508 of the Rehabilitation Act of 1973, as amended, and 29 U.S.C. s. 794(d), including the regulations set forth under 36 C.F.R. part

1194, except when compliance with this section imposes an undue burden; however, in such instance, a state agency must provide individuals with disabilities with the information and data involved by an alternative method of access that allows the individual to use the information and data.

(2) This section does not require a state agency to install specific accessibility-related software or attach an assistive technology device at a work station of a state employee who is not an individual with a disability.

(3) This section does not require a state agency, when providing the public with access to information or data through electronic information technology, to make products owned by the state agency available for access and use by individuals with disabilities at a location other than the location at which the electronic information and information technology are normally provided to the public. This section does not require a state agency to purchase products for access and use by individuals with disabilities at a location other than at the location where the electronic information and information technology are normally provided to the public.

History.—s. 73, ch. 2006-227.

282.604 Adoption of rules.— The Department of Management Services shall, with input from stakeholders, adopt rules pursuant to ss. 120.536(1) and 120.54 for the development, procurement, maintenance, and use of accessible electronic information technology by governmental units.

History.—s. 73, ch. 2006-227.

282.605 Exceptions.—

(1) This part does not apply to electronic information and information technology of the Department of Military Affairs or the Florida National Guard if the function, operation, or use of the information or technology involves intelligence activities or cryptologic activities related to national security, the command and control of military forces, equipment that is an integral part of a weapon or weapons system, or systems that are critical to the direct fulfillment of military or intelligence missions. Systems that are critical to the direct fulfillment of military or intelligence missions do not include a system that is used for routine administrative and business applications, including, but not limited to, payroll, finance, logistics, and personnel management applications.

(2) This part does not apply to electronic information and information technology of a state agency if the function, operation, or use of the information or technology involves criminal intelligence activities. Such activities do not include information or technology that is used for routine administrative and business applications, including, but not limited to, payroll, finance, logistics, and personnel management applications.

(3) This part does not apply to electronic information and information technology that is acquired by a contractor and that is incidental to the contract.

(4) This part applies to competitive solicitations issued or new systems developed by a state agency on or after July 1, 2006.

History.—s. 73, ch. 2006-227.

282.606 Intent.— It is the intent of the Legislature that, in construing this part, due consideration and great weight be given to the interpretations of the federal courts relating to comparable provisions of s. 508 of the Rehabilitation Act of 1973, as amended, and 29 U.S.C. s. 794(d), including the regulations set forth under 36 C.F.R. part 1194, as of July 1, 2006.

History.—s. 73, ch. 2006-227.

PART III
COMMUNICATION INFORMATION TECHNOLOGY SERVICES

282.701 Short title.—This part may be cited as the "Communication Information Technology Services Act."

History.—s. 16, ch. 2009-80.

282.702 Powers and duties.—The Department of Management Services shall have the following powers, duties, and functions:

(1) To publish electronically the portfolio of services available from the department, including pricing information; the policies and procedures governing usage of available services; and a forecast of the department's priorities for each telecommunications service.

(2) To adopt technical standards by rule for the state telecommunications network which ensure the interconnection and operational security of computer networks, telecommunications, and information systems of agencies.

(3) To enter into agreements related to information technology and telecommunications services with state agencies and political subdivisions of the state.

(4) To purchase from or contract with information technology providers for information technology, including private line services.

(5) To apply for, receive, and hold authorizations, patents, copyrights, trademarks, service marks, licenses, and allocations or channels and frequencies to carry out the purposes of this part.

(6) To purchase, lease, or otherwise acquire and to hold, sell, transfer, license, or otherwise dispose of real, personal, and intellectual property, including, but not limited to, patents, trademarks, copyrights, and service marks.

(7) To cooperate with any federal, state, or local emergency management agency in providing for emergency telecommunications services.

(8) To control and approve the purchase, lease, or acquisition and the use of telecommunications services, software, circuits, and equipment provided as part of any other total telecommunications system to be used by the state or its agencies.

(9) To adopt rules pursuant to ss. 120.536(1) and 120.54 relating to telecommunications and to administer the provisions of this part.

(10) To apply for and accept federal funds for the purposes of this part as well as gifts and donations from individuals, foundations, and private organizations.

(11) To monitor issues relating to telecommunications facilities and services before the Florida Public Service Commission and the Federal Communications Commission and, if necessary, prepare position papers, prepare testimony, appear as a witness, and retain witnesses on behalf of state agencies in proceedings before the commissions.

(12) Unless delegated to the agencies by the department, to manage and control, but not intercept or interpret, telecommunications within the SUNCOM Network by:

(a) Establishing technical standards to physically interface with the SUNCOM Network.

(b) Specifying how telecommunications are transmitted within the SUNCOM Network.

(c) Controlling the routing of telecommunications within the SUNCOM Network.

(d) Establishing standards, policies, and procedures for access to and the security of the SUNCOM Network.

(e) Ensuring orderly and reliable telecommunications services in accordance with the service level agreements executed with state agencies.

(13) To plan, design, and conduct experiments for telecommunications services, equipment, and technologies, and to implement enhancements in the state telecommunications network if in the public interest and cost-effective. Funding for such experiments must be derived from SUNCOM Network service revenues and may not exceed 2 percent of the annual budget for the SUNCOM Network for any fiscal year or as provided in the General Appropriations Act. New services offered as a result of this subsection may not affect existing rates for facilities or services.

(14) To enter into contracts or agreements, with or without competitive bidding or procurement, to make available, on a fair, reasonable, and nondiscriminatory basis, property and other structures under departmental control for the placement of new facilities by any wireless provider of mobile service as defined in 47 U.S.C. s. 153(27) or s. 332(d) and any telecommunications company as defined in s. 364.02 if it is practical and feasible to make such property or other structures available. The department may, without adopting a rule, charge a just, reasonable, and nondiscriminatory fee for the placement of the facilities, payable annually, based on the fair market value of space used by comparable telecommunications facilities in the state. The department and a wireless provider or telecommunications company may negotiate the reduction or elimination of a fee in consideration of services provided to the department by the wireless provider or telecommunications company. All such fees collected by the department shall be deposited directly into the Law Enforcement Radio Operating Trust Fund, and may be used by the department to construct, maintain, or support the system.

(15) Establish policies that ensure that the department's cost-recovery methodologies, billings, receivables, expenditures, budgeting, and accounting data are captured and reported timely, consistently, accurately, and transparently and are in compliance with all applicable federal and state laws and rules. The department shall annually submit to the Governor, the President of the Senate, and the Speaker of the House of Representatives a report that describes each service and its cost, the billing methodology for recovering the cost of the service, and, if applicable, the identity of those services that are subsidized.

History.—s. 22, ch. 69-106; s. 1, ch. 70-327; s. 36, ch. 83-334; s. 11, ch. 87-137; s. 220, ch. 92-279; s. 55, ch. 92-326; s. 16, ch. 95-143; s. 1, ch. 96-357; s. 9, ch. 96-390; s. 11, ch. 97-286; s. 65, ch. 98-279; s. 5, ch. 2000-164; s. 11, ch. 2001-261; s. 36, ch. 2002-1; s. 18, ch. 2007-105; s. 17, ch. 2009-80; s. 48, ch. 2010-5; s. 10, ch. 2010-148.

Note.—Former s. 287.25; s. 282.102.

282.703 SUNCOM Network; exemptions from the required use.—

(1) The SUNCOM Network is established within the department as the state enterprise telecommunications system for providing local and long-distance communications services to state agencies, political subdivisions of the state, municipalities, and nonprofit corporations pursuant to this part. The SUNCOM Network shall be developed to transmit all types of telecommunications signals, including, but not limited to, voice, data, video, image, and radio. State agencies shall cooperate and assist in the development and joint use of telecommunications systems and services.

(2) The department shall design, engineer, implement, manage, and operate through state ownership, commercial leasing, contracted services, or some combination thereof, the facilities, equipment, and contracts providing SUNCOM Network services, and shall develop a system of equitable billings and charges for telecommunications services.

(3) The department shall own, manage, and establish standards for the telecommunications addressing and numbering plans for the SUNCOM Network. This includes distributing or revoking numbers and addresses to authorized users of the network and delegating or revoking the delegation of management of subsidiary groups of numbers and addresses to authorized users of the network.

(4) The department shall maintain a directory of information and services which provides the names, phone numbers, and e-mail addresses for employees, agencies, and network devices that are served, in whole or in part, by the SUNCOM Network. State agencies and political subdivisions of the state shall cooperate with the department by providing timely and accurate directory information in the manner established by the department.

(5) All state agencies shall use the SUNCOM Network for agency telecommunications services as the services become available; however, an agency is not relieved of responsibility for maintaining telecommunications services

necessary for effective management of its programs and functions. The department may provide such communications services to a state university if requested by the university.

(a) If a SUNCOM Network service does not meet the telecommunications requirements of an agency, the agency must notify the department in writing and detail the requirements for that service. If the department is unable to meet an agency's requirements by enhancing SUNCOM Network service, the department may grant the agency an exemption from the required use of specified SUNCOM Network services.

(b) Unless an exemption has been granted by the department, effective October 1, 2010, all customers of a state primary data center, excluding state universities, must use the shared SUNCOM Network telecommunications services connecting the state primary data center to SUNCOM services for all telecommunications needs in accordance with department rules.

1. Upon discovery of customer noncompliance with this paragraph, the department shall provide the affected customer with a schedule for transferring to the shared telecommunications services provided by the SUNCOM Network and an estimate of all associated costs. The state primary data centers and their customers shall cooperate with the department to accomplish the transfer.

2. Customers may request an exemption from this paragraph in the same manner as authorized in paragraph (a).

(6) This section may not be construed to require a state university to use SUNCOM Network communication services.

History.—s. 22, ch. 69-106; s. 13, ch. 87-137; s. 3, ch. 91-171; s. 222, ch. 92-279; s. 55, ch. 92-326; s. 10, ch. 96-390; s. 66, ch. 98-279; s. 6, ch. 2000-164; s. 12, ch. 2001-261; s. 935, ch. 2002-387; s. 19, ch. 2007-105; s. 18, ch. 2009-80; s. 6, ch. 2010-78; s. 11, ch. 2010-148.

Note.—Former s. 287.27; s. 282.103.

282.704 Use of state SUNCOM Network by municipalities.—Any municipality may request the department to provide any or all of the SUNCOM Network's portfolio of communications services upon such terms and conditions as the department may establish. The requesting municipality shall pay its share of installation and recurring costs according to the published rates for SUNCOM Network services and as invoiced by the department. Such municipality shall also pay for any requested modifications to existing SUNCOM Network services, if any charges apply.

History.—s. 3, ch. 82-56; s. 1, ch. 83-70; s. 14, ch. 87-137; s. 11, ch. 96-390; s. 67, ch. 98-279; s. 7, ch. 2000-164; s. 13, ch. 2001-261; s. 19, ch. 2009-80.

Note.—Former s. 287.251; s. 282.104.

282.705 Use of state SUNCOM Network by nonprofit corporations.—

(1) The department shall provide a means whereby private nonprofit corporations under contract with state agencies or political subdivisions of the state may use the state SUNCOM Network, subject to the limitations in this section. In order to qualify to use the state SUNCOM Network, a nonprofit corporation shall:

(a) Expend the majority of its total direct revenues for the provision of contractual services to the state, a municipality, or a political subdivision; and

(b) Receive only a small portion of its total revenues from any source other than a state agency, a municipality, or a political subdivision during the time SUNCOM Network services are requested.

(2) Each nonprofit corporation seeking authorization to use the state SUNCOM Network shall provide to the department, upon request, proof of compliance with subsection (1).

(3) Nonprofit corporations established pursuant to general law and an association of municipal governments which is wholly owned by the municipalities are eligible to use the state SUNCOM Network, subject to the terms and conditions of the department.

(4) Institutions qualified to participate in the William L. Boyd, IV, Effective Access to Student Education Grant Program pursuant to s. 1009.89 are eligible to use the state SUNCOM Network, subject to the terms and conditions of the department. Such entities are not required to satisfy the other criteria of this section.

(5) Private, nonprofit elementary and secondary schools are eligible for rates and services on the same basis as public schools if such schools do not have an endowment in excess of $50 million.

History.—s. 1, ch. 80-107; s. 2, ch. 82-56; s. 3, ch. 83-70; s. 15, ch. 87-137; s. 223, ch. 92-279; s. 55, ch. 92-326; s. 197, ch. 95-148; s. 12, ch. 96-390; s. 19, ch. 97-296; s. 68, ch. 98-279; s. 36, ch. 99-399; s. 8, ch. 2000-164; s. 14, ch. 2001-261; s. 936, ch. 2002-387; s. 20, ch. 2009-80; s. 25, ch. 2018-4; s. 42, ch. 2019-3.

Note.—Former s. 287.272; s. 282.105.

282.706 Use of SUNCOM Network by libraries.—The department may provide SUNCOM Network services to any library in the state, including libraries in public schools, community colleges, state universities, and nonprofit private postsecondary educational institutions, and libraries owned and operated by municipalities and political subdivisions. This section may not be construed to require a state university library to use SUNCOM Network services.

History.—s. 2, ch. 96-357; s. 9, ch. 2000-164; s. 15, ch. 2001-261; s. 937, ch. 2002-387; s. 21, ch. 2009-80; s. 7, ch. 2010-78.

Note.—Former s. 282.106.

282.707 SUNCOM Network; criteria for usage.—

(1) The department and customers served by the department shall periodically review the qualifications of subscribers using the state SUNCOM Network and terminate services provided to a facility not qualified under this part or rules adopted hereunder. In the event of nonpayment of invoices by subscribers whose SUNCOM Network invoices are paid from sources other than legislative appropriations, such nonpayment represents good and sufficient reason to terminate service.

(2) The department shall adopt rules for implementing and operating the state SUNCOM Network, which include procedures for withdrawing and restoring authorization to use the state SUNCOM Network. Such rules shall provide a minimum of 30 days' notice to affected parties before terminating voice communications service.

(3) This section does not limit or restrict the ability of the Florida Public Service Commission to set jurisdictional tariffs of telecommunications companies.

History.—s. 1, ch. 82-56; s. 2, ch. 83-70; s. 16, ch. 87-137; s. 13, ch. 96-390; s. 33, ch. 2000-152; s. 10, ch. 2000-164; s. 20, ch. 2007-105; s. 22, ch. 2009-80; s. 12, ch. 2010-148.

Note.—Former s. 287.255; s. 282.107.

282.708 Emergency assumption of control.—In the event of an emergency, the Governor may direct emergency management assumption of control over all or part of the state communications system.

History.—s. 22, ch. 69-106; s. 37, ch. 83-334; s. 23, ch. 2009-80.

Note.—Former s. 287.28; s. 282.109.

282.709 State agency law enforcement radio system and interoperability network.—

(1) The department may acquire and administer a statewide radio communications system to serve law enforcement units of state agencies, and to serve local law enforcement agencies through mutual aid channels.

(a) The department shall, in conjunction with the Department of Law Enforcement and the Division of Emergency Management, establish policies, procedures, and standards to be incorporated into a comprehensive management plan for the use and operation of the statewide radio communications system.

(b) The department shall bear the overall responsibility for the design, engineering, acquisition, and implementation of the statewide radio communications system and for ensuring the proper operation and maintenance of all common system equipment.

(c)1. The department may rent or lease space on any tower under its control and refuse to lease space on any tower at any site.

2. The department may rent, lease, or sublease ground space as necessary to locate equipment to support antennae on the towers. The costs for the use of such space shall be established by the department for each site if it is determined to be practicable and feasible to make space available.

3. The department may rent, lease, or sublease ground space on lands acquired by the department for the construction of privately owned or publicly owned towers. The department may, as a part of such rental, lease, or

sublease agreement, require space on such towers for antennae as necessary for the construction and operation of the state agency law enforcement radio system or any other state need.

4. All moneys collected by the department for rents, leases, and subleases under this subsection shall be deposited directly into the State Agency Law Enforcement Radio System Trust Fund established in subsection (3) and may be used by the department to construct, maintain, or support the system.

5. The positions necessary for the department to accomplish its duties under this subsection shall be established in the General Appropriations Act and funded by the Law Enforcement Radio Operating Trust Fund or other revenue sources.

(d) The department shall exercise its powers and duties under this part to plan, manage, and administer the mutual aid channels in the statewide radio communication system.

1. In implementing such powers and duties, the department shall consult and act in conjunction with the Department of Law Enforcement and the Division of Emergency Management, and shall manage and administer the mutual aid channels in a manner that reasonably addresses the needs and concerns of the involved law enforcement agencies and emergency response agencies and entities.

2. The department may make the mutual aid channels available to federal agencies, state agencies, and agencies of the political subdivisions of the state for the purpose of public safety and domestic security.

(e) The department may allow other state agencies to use the statewide radio communications system under terms and conditions established by the department.

(2) The Joint Task Force on State Agency Law Enforcement Communications is created adjunct to the department to advise the department of member-agency needs relating to the planning, designing, and establishment of the statewide communication system.

(a) The Joint Task Force on State Agency Law Enforcement Communications shall consist of the following members:

1. A representative of the Division of Alcoholic Beverages and Tobacco of the Department of Business and Professional Regulation who shall be appointed by the secretary of the department.

2. A representative of the Division of Florida Highway Patrol of the Department of Highway Safety and Motor Vehicles who shall be appointed by the executive director of the department.

3. A representative of the Department of Law Enforcement who shall be appointed by the executive director of the department.

4. A representative of the Fish and Wildlife Conservation Commission who shall be appointed by the executive director of the commission.

5. A representative of the Division of Law Enforcement of the Department of Environmental Protection who shall be appointed by the secretary of the department.

6. A representative of the Department of Corrections who shall be appointed by the secretary of the department.

7. A representative of the Department of Financial Services who shall be appointed by the Chief Financial Officer.

8. A representative of the Department of Agriculture and Consumer Services who shall be appointed by the Commissioner of Agriculture.

9. A representative of the Florida Sheriffs Association who shall be appointed by the president of the Florida Sheriffs Association.

(b) Each appointed member of the joint task force shall serve at the pleasure of the appointing official. Any vacancy on the joint task force shall be filled in the same manner as the original appointment. A joint task force member may, upon notification to the chair before the beginning of any scheduled meeting, appoint an alternative to represent the member on the task force and vote on task force business in his or her absence.

(c) The joint task force shall elect a chair from among its members to serve a 1-year term. A vacancy in the chair of the joint task force must be filled for the remainder of the unexpired term by an election of the joint task force members.

(d) The joint task force shall meet as necessary, but at least quarterly, at the call of the chair and at the time and place designated by him or her.

(e) The per diem and travel expenses incurred by a member of the joint task force who represents a state agency in attending task force meetings and in attending to task force affairs shall be paid pursuant to s. 112.061, from funds budgeted to the state agency that the member represents. The per diem and travel expenses incurred by the member of the task force who represents the Florida Sheriffs Association in attending task force meetings and in attending to task force affairs shall be paid pursuant to s. 112.061, by the sheriff's office that employs the representative.

(f) The department shall provide technical support to the joint task force.

[1](3) In recognition of the critical nature of the statewide law enforcement radio communications system, the Legislature finds that there is an immediate danger to the public health, safety, and welfare, and that it is in the best interest of the state to continue partnering with the system's current operator. The Legislature finds that continuity of coverage is critical to supporting law enforcement, first responders, and other public safety users. The potential for a loss in coverage or a lack of interoperability between users requires emergency action and is a serious concern for officers' safety and their ability to communicate and respond to various disasters and events.

(a) The department, pursuant to s. 287.057(11), shall enter into a 15-year contract with the entity that was operating the statewide radio communications system on January 1, 2021. The contract must include:

1. The purchase of radios;
2. The upgrade to the Project 25 communications standard;
3. Increased system capacity and enhanced coverage for system users;
4. Operations, maintenance, and support at a fixed annual rate;
5. The conveyance of communications towers to the department; and
6. The assignment of communications tower leases to the department.

(b) The State Agency Law Enforcement Radio System Trust Fund is established in the department and funded from surcharges collected under ss. 318.18, 320.0802, and 328.72. Upon appropriation, moneys in the trust fund may be used by the department to acquire the equipment, software, and engineering, administrative, and maintenance services it needs to construct, operate, and maintain the statewide radio system. Moneys in the trust fund from surcharges shall be used to help fund the costs of the system. Upon completion of the system, moneys in the trust fund may also be used by the department for payment of the recurring maintenance costs of the system.

(4) The department may create and administer an interoperability network to enable interoperability between various radio communications technologies and to serve federal agencies, state agencies, and agencies of political subdivisions of the state for the purpose of public safety and domestic security.

(a) The department shall, in conjunction with the Department of Law Enforcement and the Division of Emergency Management, exercise its powers and duties pursuant to this chapter to plan, manage, and administer the interoperability network. The office may:

1. Enter into mutual aid agreements among federal agencies, state agencies, and political subdivisions of the state for the use of the interoperability network.
2. Establish the cost of maintenance and operation of the interoperability network and charge subscribing federal and local law enforcement agencies for access and use of the network. The department may not charge state law enforcement agencies identified in paragraph (2)(a) to use the network.
3. In consultation with the Department of Law Enforcement and the Division of Emergency Management, amend and enhance the statewide radio communications system as necessary to implement the interoperability network.

(b) The department, in consultation with the Joint Task Force on State Agency Law Enforcement Communications, and in conjunction with the Department of Law Enforcement and the Division of Emergency Management, shall establish policies, procedures, and standards to incorporate into a comprehensive management plan for the use and operation of the interoperability network.

History.—s. 1, ch. 88-144; s. 1, ch. 92-72; s. 224, ch. 92-279; s. 55, ch. 92-326; s. 30, ch. 94-218; s. 111, ch. 94-356; s. 860, ch. 95-148; s. 5, ch. 95-283; s. 1, ch. 96-312; s. 5, ch. 96-357; s. 10, ch. 96-388; s. 14, ch. 96-390; s. 6, ch. 98-251; s. 69, ch. 98-279; s. 81, ch. 99-245; s. 3, ch. 99-289; s. 37, ch. 99-399; s. 11, ch. 2000-164; s. 16, ch. 2001-261; s. 2, ch. 2003-153; s. 308, ch. 2003-261; s. 24, ch. 2009-80; s. 24, ch. 2011-47; s. 125, ch. 2011-142; s. 10, ch. 2012-88; s. 21, ch. 2012-119; s. 5, ch. 2014-18; ss. 29, 30, 66, ch. 2014-53; s. 4, ch. 2014-150; ss. 42, 43, ch. 2015-222; ss. 71, 72, ch. 2016-62; s. 27,

ch. 2016-165; s. 26, ch. 2017-71; s. 1, ch. 2018-67; s. 9, ch. 2019-141; ss. 69, 70, ch. 2021-37; ss. 53, 54, ch. 2022-157; ss. 42, 43, ch. 2023-240; ss. 52, 53, ch. 2024-228.

[1]**Note.**—

A. Section 52, ch. 2024-228, reenacted and amended subsection (3) "[i]n order to implement Specific Appropriation 2991 of the 2024-2025 General Appropriations Act."

B. Section 53, ch. 2024-228, provides that "[t]he text of s. 282.709(3), Florida Statutes, as carried forward from chapter 2021-37, Laws of Florida, by this act, expires July 1, 2025, and the text of that subsection shall revert to that in existence on June 1, 2021, except that any amendments to such text enacted other than by this act shall be preserved and continue to operate to the extent that such amendments are not dependent upon the portions of text which expire pursuant to this section." Effective July 1, 2025, subsection (3), as amended by section 53, ch. 2024-228, will read:

(3) The State Agency Law Enforcement Radio System Trust Fund is established in the department and funded from surcharges collected under ss. 318.18, 320.0802, and 328.72. Upon appropriation, moneys in the trust fund may be used by the department to acquire by competitive procurement the equipment, software, and engineering, administrative, and maintenance services it needs to construct, operate, and maintain the statewide radio system. Moneys in the trust fund from surcharges shall be used to help fund the costs of the system. Upon completion of the system, moneys in the trust fund may also be used by the department for payment of the recurring maintenance costs of the system.

Note.—Former s. 282.1095.

282.7101 Statewide system of regional law enforcement communications.—

(1) It is the intent and purpose of the Legislature that a statewide system of regional law enforcement communications be developed whereby maximum efficiency in the use of existing radio channels is achieved in order to deal more effectively with the apprehension of criminals and the prevention of crime. To this end, all law enforcement agencies within the state are directed to provide the department with any information the department requests for the purpose of implementing the provisions of subsection (2).

(2) The department is hereby authorized and directed to develop and maintain a statewide system of regional law enforcement communications. In formulating such a system, the department shall divide the state into appropriate regions and shall develop a program that includes, but is not limited to:

(a) The communications requirements for each county and municipality comprising the region.

(b) An interagency communications provision that depicts the communication interfaces between municipal, county, and state law enforcement entities operating within the region.

(c) A frequency allocation and use provision that includes, on an entity basis, each assigned and planned radio channel and the type of operation, simplex, duplex, or half-duplex, on each channel.

(3) The department shall adopt any necessary rules and regulations for administering and coordinating the statewide system of regional law enforcement communications.

(4) The secretary of the department or his or her designee is designated as the director of the statewide system of regional law enforcement communications and, for the purpose of carrying out the provisions of this section, may coordinate the activities of the system with other interested state agencies and local law enforcement agencies.

(5) A law enforcement communications system may not be established or expanded without the prior approval of the department.

(6) Within the limits of its capability, the Department of Law Enforcement is encouraged to lend assistance to the department in the development of the statewide system of regional law enforcement communications proposed by this section.

History.—ss. 1, 2, 3, 4, 5, 6, ch. 72-296; s. 1, ch. 77-174; s. 12, ch. 79-8; s. 225, ch. 92-279; s. 55, ch. 92-326; s. 11, ch. 96-388; s. 15, ch. 96-390; s. 7, ch. 98-251; s. 70, ch. 98-279; s. 42, ch. 99-399; s. 12, ch. 2000-164; s. 17, ch. 2001-261; s. 25, ch. 2009-80.

Note.—Former s. 287.29; s. 282.111.

282.711 Remote electronic access services.—The department may collect fees for providing remote electronic access pursuant to s. 119.07(2). The fees may be imposed on individual transactions or as a fixed subscription for a designated period of time. All fees collected under this section shall be deposited in the appropriate trust fund of the program or activity that made the remote electronic access available.

History.—s. 13, ch. 97-241; s. 14, ch. 2000-164; s. 19, ch. 2001-261; s. 37, ch. 2004-335; s. 26, ch. 2009-80.

Note.—Former s. 282.21.

282.802 Government Technology Modernization Council.—

(1) The Government Technology Modernization Council, an advisory council as defined in s. 20.03(7), is created within the department. Except as otherwise provided in this section, the advisory council shall operate in a manner consistent with s. 20.052.

(2) The purpose of the council is to study and monitor the development and deployment of new technologies and provide reports on recommendations for procurement and regulation of such systems to the Governor, the President of the Senate, and the Speaker of the House of Representatives.

(3) The council shall be composed of the following members:

(a) The Lieutenant Governor as chair.

(b) The state chief information officer.

(c) The Secretary of Commerce or his or her designee.

(d) The Secretary of Health Care Administration or his or her designee.

(e) The Secretary of Transportation or his or her designee.

(f) The executive director of the Department of Law Enforcement or his or her designee.

(g) Five representatives with senior level experience or expertise in artificial intelligence, cloud computing, identity management, data science, machine learning, government procurement, financial technology, education technology, and constitutional law, with three appointed by the Governor, one appointed by the President of the Senate, and one appointed by the Speaker of the House of Representatives.

(h) One member of the Senate, appointed by the President of the Senate.

(i) One member of the House of Representatives, appointed by the Speaker of the House of Representatives.

(4) Members shall serve for terms of 4 years, except that sitting members of the Senate and the House of Representatives shall serve terms that correspond with their terms of office. For the purpose of providing staggered terms, the initial appointments of members made by the Governor shall be for terms of 2 years. A vacancy shall be filled for the remainder of the unexpired term in the same manner as the initial appointment. All members of the council are eligible for reappointment.

(5) The Secretary of Management Services, or his or her designee, shall serve as the ex officio, nonvoting executive director of the council.

(6) Members of the council shall serve without compensation but are entitled to receive reimbursement for per diem and travel expenses pursuant to s. 112.061.

(7)(a) The council shall meet at least quarterly to:

1. Recommend legislative and administrative actions that the Legislature and state agencies as defined in s. 282.318(2) may take to promote the development of data modernization in this state.

2. Assess and provide guidance on necessary legislative reforms and the creation of a state code of ethics for artificial intelligence systems in state government.

3. Assess the effect of automated decision systems or identity management on constitutional and other legal rights, duties, and privileges of residents of this state.

4. Evaluate common standards for artificial intelligence safety and security measures, including the benefits of requiring disclosure of the digital provenance for all images and audio created using generative artificial intelligence as a means of revealing the origin and edit of the image or audio, as well as the best methods for such disclosure.

5. Assess the manner in which governmental entities and the private sector are using artificial intelligence with a focus on opportunity areas for deployments in systems across this state.

6. Determine the manner in which artificial intelligence is being exploited by bad actors, including foreign countries of concern as defined in s. 287.138(1).

7. Evaluate the need for curriculum to prepare school-age audiences with the digital media and visual literacy skills needed to navigate the digital information landscape.

(b) At least one quarterly meeting of the council must be a joint meeting with the Florida Cybersecurity Advisory Council.

(8) By December 31, 2024, and each December 31 thereafter, the council shall submit to the Governor, the President of the Senate, and the Speaker of the House of Representatives any legislative recommendations considered necessary by the council to modernize government technology, including:

(a) Recommendations for policies necessary to:

1. Accelerate adoption of technologies that will increase productivity of state enterprise information technology systems, improve customer service levels of government, and reduce administrative or operating costs.

2. Promote the development and deployment of artificial intelligence systems, financial technology, education technology, or other enterprise management software in this state.

3. Protect Floridians from bad actors who use artificial intelligence.

(b) Any other information the council considers relevant.

History.—s. 1, ch. 2024-118.