A bill to be entitled

An act relating to information technology; providing for a type two transfer of the specified functions and components of the Florida Digital Service to the Executive Office of the Governor; providing for the continuation of certain contracts and interagency agreements; providing that all functions, records, personnel, contracts, interagency agreements, and equipment of the Department of Management Services State Data Center are consolidated in the Northwest Regional Data Center; transferring remaining funds from the Working Capital Trust Fund to the Northwest Regional Data Center for specified purposes; creating s. 14.2017, F.S.; creating the Enterprise Florida First Technology Center within the Executive Office of the Governor; providing for the management of the center by a director; prescribing qualifications of the director and state chief data officer; providing that the center is a separate budget entity; prescribing duties of the director; amending s. 20.22, F.S.; removing the Florida Digital Service from the divisions, programs, and services within the Department of Management Services, to conform to changes made by the act; amending s. 282.0041, F.S.; revising the definition of the term "service-level agreement"; amending s. 282.0051, F.S.; creating the Enterprise Florida First Technology Center within the Executive Office of the Governor; deleting references to the Florida Digital Service to conform to changes

made by the act; requiring the center to consult with the Department of Management Services to establish an information technology policy for specified procurement activities; requiring the Enterprise Florida First Technology Center to adopt rules; conforming provisions to changes made by the act; repealing s. 282.201, F.S., relating to the state data center; amending s. 282.318, F.S.; designating the Enterprise Florida First Technology Center as the lead entity in state agency cybersecurity matters; requiring the center to adopt certain rules; requiring the center to designate an employee as the state chief information security officer; conforming provisions to changes made by the act; amending s. 282.319, F.S.; housing the Florida Cybersecurity Advisory Council within the Executive Office of the Governor, rather than the Department of Management Services, to conform to changes made by the act; providing that the director of the Office of Policy and Budget, rather than the Secretary of Management Services, is the executive director of the advisory council; conforming provisions to changes made by the act; amending s. 287.0591, F.S.; requiring the Enterprise Florida First Technology Center to participate in certain solicitations for information technology commodities and services; requiring the Department of Management Services to consult with the Enterprise Florida First Technology Center in prequalifying entities to provide information technology services to the state; amending

s. 1004.649, F.S.; designating the Northwest Regional Data Center as the state data center; specifying required duties of the Northwest Regional Data Center; specifying additional requirements for service-level agreements with state agency customers; exempting certain entities from using the data center; prohibiting state agencies from engaging in certain activities, unless otherwise authorized; modifying provisions governing the transition of state agency customers to a cloud-based data center; amending ss. 282.00515, 443.1113, and 943.0415, F.S.; conforming a cross-reference and provisions to changes made by the act; providing an effective date.

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

Section 1. All powers; duties; functions; records; offices; personnel; associated administrative support positions; property; pending issues and existing contracts; administrative authority; administrative rules in chapter 74, Florida Administrative Code, in effect as of July 1, 2022; and unexpended balances of appropriations and allocations from the General Revenue Fund of the Department of Management Services Florida Digital Service, with the exception of the State Data Center, are transferred by a type two transfer pursuant to s. 20.06(2), Florida Statutes, to the Executive Office of the Governor.

Section 2. Any contract or interagency agreement existing before July 1, 2022, between the Department of Management

Services Florida Digital Service, or any entity or agent of the agency, and any other agency, entity, or person shall continue as a contract or agreement of the successor department or entity responsible for the program, activity, or function relative to the contract or agreement.

Section 3. All functions, records, personnel, contracts, interagency agreements, and equipment in the current Department of Management Services State Data Center are consolidated in the Northwest Regional Data Center. The unexpended balance of funds remaining in the Working Capital Trust Fund on June 30, 2022, is transferred to the Northwest Regional Data Center to be used to satisfy customer refunds or excess assessments for fiscal year 2021-2022.

Section 4. Section 14.2017, Florida Statutes, is created to read:

14.2017 Enterprise Florida First Technology Center.—

(1) The Enterprise Florida First Technology Center is established within the Executive Office of the Governor, headed for all purposes by a director who holds the title of state chief information officer. The Enterprise Florida First Technology Center shall be a separate budget entity. The director of the center shall be appointed by and serves at the pleasure of the Governor and must be a proven, effective administrator who has at least 10 years of executive-level experience in the public or private sector, preferably with experience in the development of information technology strategic planning and the development and implementation of fiscal and substantive information technology policy and standards.

(2) The state chief information officer 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 state chief information officer shall facilitate meetings with all state agency chief information officers for the purpose of communication regarding standards, rules, projects, and significant events related to information technology. These meetings must be held at least quarterly.

Section 5. Paragraph (b) of subsection (2) of section 20.22, Florida Statutes, is amended to read:

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

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

~~(b) The Florida Digital Service.~~

Section 6. Subsection (30) of section 282.0041, Florida Statutes, is amended to read:

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

(30) "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, service level, the duration of the agreement, the responsible parties, and service costs. A service-level agreement is not a rule pursuant to chapter 120.

Section 7. Section 282.0051, Florida Statutes, is amended to read:

282.0051 Executive Office of the Governor ~~Department of~~

~~Management Services~~; Enterprise Florida First Technology Center ~~Florida Digital Service~~; powers, duties, and functions.—

(1) The Enterprise Florida First Technology Center ~~Florida Digital Service~~ has been created within the Executive Office of the Governor ~~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 Executive Office of the Governor ~~department~~, through the Enterprise Florida First Technology Center ~~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 center ~~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 center ~~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 center ~~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 center ~~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 center ~~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) ~~Provide operational management and oversight of the~~

~~state data center established pursuant to s. 282.201, which includes:~~

~~1. Implementing industry standards and best practices for the state data center's facilities, operations, maintenance, planning, and management processes.~~

~~2. 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 Florida Digital Service 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 mechanism may be implemented only if specifically authorized by the Legislature.~~

~~3. Developing and implementing appropriate operating guidelines and procedures necessary for the state data center to perform its duties pursuant to s. 282.201. The guidelines and procedures must comply with applicable state and federal laws, regulations, and policies and conform to generally accepted governmental accounting and auditing standards. The guidelines and procedures must include, but need not be limited to:~~

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

~~b. Implementing an annual reconciliation process to ensure~~

~~that each customer entity is paying for the full direct and indirect cost of each service as determined by the customer entity's use of each service.~~

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

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

~~e. 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.~~

~~f. 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 sub-subparagraph d. Such a plan is required only if the service cost increase results in a net increase to a customer entity for that fiscal year.~~

~~g. Standardizing and consolidating procurement and contracting practices.~~

~~4.~~ Collaborate ~~In collaboration~~ with the Department of Law Enforcement, to develop and implement ~~developing and implementing~~ a process for detecting, reporting, and responding to cybersecurity incidents, breaches, and threats.

~~5. 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.~~

(k) 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.

(l) 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.

(m) 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.

(n)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 center ~~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 center ~~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 must ~~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.

(o) 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.

(p) 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 center ~~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.

(q)1. Establish, in consultation with the department, 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 (n), 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.

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

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

(t) 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 Enterprise Florida First Technology Center ~~department, acting through the Florida Digital Service and~~ from funds appropriated to the center ~~Florida Digital Service~~, shall:

(a) Create, not later than December 1, 2022 ~~October 1,~~

~~2021~~, 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 ~~October 1, 2021~~, 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.

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

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

(b) The center ~~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 center ~~Florida Digital Service~~ must participate in post-award contract monitoring.

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

(5) ~~(6)~~ The Enterprise Florida First Technology Center ~~department, acting through the Florida Digital Service,~~ shall adopt rules to administer this section.

Section 8. Section 282.201, Florida Statutes, is repealed.

Section 9. Subsections (3), (4), (8), and (11) of section 282.318, Florida Statutes, are amended to read:

282.318 Cybersecurity.—

(3) The Enterprise Florida First Technology Center ~~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 Enterprise Florida First Technology Center ~~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 center ~~department, acting through the Florida Digital Service,~~ shall also:

(a) Designate an employee of the center ~~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 center ~~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 and tiered reporting timeframes for notifying the center ~~department~~ and the Department of Law Enforcement of cybersecurity incidents. The tiered reporting timeframes shall be based upon the level of severity of the cybersecurity incidents being reported.

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.

(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) Provide cybersecurity training to all state agency technology professionals that develops, assesses, and documents competencies by role and skill level. 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 Enterprise Florida First Technology Center ~~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 center ~~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 Executive Office of the Governor ~~department~~ annually by July 31, the state agency's strategic and operational cybersecurity plans developed pursuant to rules and guidelines established by the center ~~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 center ~~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 center ~~department~~ and is confidential and exempt from s. 119.07(1), except that such information shall be available to the Auditor General, the center ~~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 center ~~Florida Digital Service within the department~~. Such policies and procedures must be consistent with the rules, guidelines, and processes established by the center ~~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 center ~~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 center ~~department~~ to address identified risks to the data, information, and information technology resources of the agency. The center ~~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 center ~~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 in the first 30 days after commencing employment 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 center ~~department through the Florida Digital Service~~.

1. All cybersecurity incidents and breaches must be reported to the center ~~Florida Digital Service within the department~~ and the Cybercrime Office of the Department of Law Enforcement and must comply with the notification procedures and reporting timeframes established pursuant to paragraph (3)(c).

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

(8) The portions of records made confidential and exempt in

subsections (5), (6), and (7) shall be available to the Auditor General, the Cybercrime Office of the Department of Law Enforcement, the center ~~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.

(11) The Enterprise Florida First Technology Center ~~department~~ shall adopt rules relating to cybersecurity and to administer this section.

Section 10. Subsections (1), (3), (6), and (9) of section 282.319, Florida Statutes, are amended to read:

282.319 Florida Cybersecurity Advisory Council.—

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

(3) The council shall assist the Enterprise Florida First Technology Center ~~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.

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

(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 Enterprise Florida First Technology Center ~~Florida Digital Service~~ in developing cybersecurity best practice recommendations for state agencies which ~~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.

Section 11. Subsections (4) and (6) of section 287.0591, Florida Statutes, are amended to read:

287.0591 Information technology; vendor disqualification.—

(4) If the department issues a competitive solicitation for information technology commodities, consultant services, or staff augmentation contractual services, the Enterprise Florida First Technology Center ~~Florida Digital Service~~ within the Executive Office of the Governor must ~~department shall~~ participate in such solicitations.

(6) Beginning October 1, 2021, and each October 1 thereafter, the department, in consultation with the Enterprise Florida First Technology Center, shall prequalify firms and individuals to provide information technology staff augmentation contractual services on state term contract. In order to

prequalify a firm or individual for participation on the state term contract, the department must consider, at a minimum, the capability, experience, and past performance record of the firm or individual. A firm or individual removed from the source of supply pursuant to s. 287.042(1)(b) or placed on a disqualified vendor list pursuant to s. 287.133 or s. 287.134 is immediately disqualified from state term contract eligibility. Once a firm or individual has been prequalified to provide information technology staff augmentation contractual services on state term contract, the firm or individual may respond to requests for quotes from an agency to provide such services.

Section 12. Section 1004.649, Florida Statutes, is amended to read:

1004.649 Northwest Regional Data Center.—

(1) The Northwest Regional Data Center is designated as the state data center and preferred cloud services provider for all state agencies. The Northwest Regional Data Center can provide data center services to state agencies from multiple facilities as funded in the General Appropriations Act.

(2) For the purpose of providing data center services to its state agency customers, the Northwest Regional Data Center shall:

(a) Operate under a governance structure that represents its customers proportionally.

(b) Maintain an appropriate cost-allocation methodology that accurately bills state agency customers based solely on the actual direct and indirect costs of the services provided to state agency customers, and ensures that for any fiscal year, state agency customers are not subsidizing other customers of

the data center. Such cost-allocation methodology must comply with applicable state and federal regulations concerning the distribution and use of state and federal funds.

(c) Enter into a service-level agreement with each state agency customer to provide services as defined and approved by the governing board of the center. At a minimum, such service-level agreements must:

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

2. State the duration of the agreement term, which may not exceed 3 years, and specify the conditions for up to two optional 1-year renewals of the agreement before execution of a new agreement ~~renewal~~;

3. Identify the scope of work;

4. Establish the services to be provided, the business standards that must be met for each service, the cost of each service, and the process by which the business standards for each service are to be objectively measured and reported;

5. Provide a timely billing methodology for recovering the cost of services provided pursuant to s. 215.422;

6. Provide a procedure for modifying the service-level agreement to address any changes in projected costs of service;

7. 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 ~~Prohibit the transfer of computing services between the Northwest Regional Data Center and the state data center established pursuant to s. 282.201 without at least 180 days' written notification of service cancellation~~;

8. Identify the products or services to be delivered with sufficient specificity to permit an external financial or performance audit; ~~and~~

9. Provide that the service-level agreement may be terminated by either party for cause only after giving the other party notice in writing of the cause for termination and an opportunity for the other party to resolve the identified cause within a reasonable period; and

10. Provide state agency customer entities with access to application, 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.

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

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

(f) Provide to the Board of Governors the total annual budget by major expenditure category, including, but not limited to, salaries, expenses, operating capital outlay, contracted services, or other personnel services by July 30 each fiscal year.

(g) ~~(e)~~ Provide to each state agency customer its projected annual cost for providing the agreed-upon data center services by September 1 each fiscal year.

(h) ~~(f)~~ Provide a plan for consideration by the Legislative Budget Commission if the governing body of the center approves the use of a billing rate schedule after the start of the fiscal year that increases any state agency customer's costs for that fiscal year.

(i) Provide data center services that comply with applicable state and federal laws, regulations, and policies, including all applicable security, privacy, and auditing requirements.

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

(3) The following entities are exempt from the requirement to use the Northwest Regional Data Center:

(a) The Department of Law Enforcement.

(b) The Department of the Lottery's Gaming System.

(c) Systems Design and Development in the Office of Policy and Budget.

(d) The regional traffic management centers described in s. 335.14(2) and the Office of Toll Operations of the Department of Transportation.

(e) The State Board of Administration.

(f) The offices of the state attorneys, public defenders, criminal conflict and regional counsels, and the capital collateral regional counsel.

(g) The Florida Housing Finance Corporation.

(4) Unless exempt from the requirement to use the Northwest Regional Data Center pursuant to this section or as authorized by the Legislature, a state agency may not do any of the following:

(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.

(b) Terminate services with the Northwest Regional Data Center without giving written notice of intent to terminate services 180 days before such termination.

(c) Procure third-party cloud-based computing services without evaluating the cloud-based computing services provided by the Northwest Regional Data Center.

(5) ~~(2)~~ The Northwest Regional Data Center's authority to provide data center services to its state agency customers may be terminated if:

(a) The center requests such termination to the Board of Governors, the Senate President, and the Speaker of the House of Representatives; or

(b) The center fails to comply with the provisions of this section.

(6) ~~(3)~~ If such authority is terminated, the center has ~~shall have~~ 1 year to provide for the transition of its state agency customers to a qualified alternative cloud-based data center that meets the enterprise architecture standards established by the Enterprise Florida First Technology Center ~~the state data center established pursuant to s. 282.201~~.

Section 13. Subsections (1) and (4) of section 282.00515, Florida Statutes, are amended to read:

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 (s) and (2)(e) ~~(3)(e)~~ or adopt alternative standards based on best practices and industry standards that allow for open data interoperability.

(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 Enterprise Florida First Technology Center ~~Florida Digital Service~~.

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

Section 14. Subsection (4) of section 443.1113, Florida Statutes, is amended to read:

443.1113 Reemployment Assistance Claims and Benefits Information System.—

(4)(a) The Department of Economic Opportunity shall perform an annual review of the system and identify enhancements or modernization efforts that improve the delivery of services to claimants and employers and reporting to state and federal

entities. These improvements must include, but need not be limited to:

1. Infrastructure upgrades through cloud services.

2. Software improvements.

3. Enhanced data analytics and reporting.

4. Increased cybersecurity pursuant to s. 282.318.

(b) The department shall seek input on recommended enhancements from, at a minimum, the following entities:

1. The Enterprise Florida First Technology Center ~~Florida Digital Service~~ within the Executive Office of the Governor ~~Department of Management Services~~.

2. The General Tax Administration Program Office within the Department of Revenue.

3. The Division of Accounting and Auditing within the Department of Financial Services.

Section 15. Subsection (5) of section 943.0415, Florida Statutes, is amended to read:

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

(5) Consult with the Enterprise Florida First Technology Center ~~Florida Digital Service~~ within the Executive Office of the Governor ~~Department of Management Services~~ in the adoption of rules relating to the information technology security provisions in s. 282.318.

Section 16. This act shall take effect July 1, 2022.