By Senator Baxley

12-01201-20 20201170__

A bill to be entitled

An act relating to public records and meetings; amending s. 282.318, F.S.; revising a provision to reflect the abolishment of the Agency for State Technology; providing an exemption from public records requirements for portions of records held by a state agency which contain network schematics, hardware and software configurations, or encryption; removing the scheduled repeal of a certain public records exemption; providing an exemption from public meetings requirements for portions of meetings which would reveal certain records; requiring the recording and transcription of exempt portions of such meetings; providing an exemption from public records requirements for such recordings and transcripts; providing an exception; revising applicability of provisions requiring and authorizing certain records to be made available to certain entities; providing for future legislative review and repeal under the Open Government Sunset Review Act of the exemptions; providing for retroactive application of the exemptions; providing statements of public necessity; providing an effective date.

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

Section 1. Section 282.318, Florida Statutes, is amended to read:

282.318 Security of data and information technology.—

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

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

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

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

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

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

1. Establishing asset management procedures to ensure that an agency's information technology resources are identified and managed consistent with their relative importance to the

agency's business objectives.

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

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

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

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

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

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

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

9. Establishing an information technology security incident reporting process that includes procedures and tiered reporting timeframes for notifying the department and the Department of

Law Enforcement of information technology security incidents. The tiered reporting timeframes shall be based upon the level of severity of the information technology security incidents being reported.

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

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

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

(d) 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 information technology security, including cybersecurity, threats, trends, and best practices.

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

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

(a) Designate an information security manager to administer the information technology security program of the state agency. This designation must be provided annually in writing to the department 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 and the Cybercrime Office of the Department of Law Enforcement, establish an agency computer security incident response team to respond to an information technology security incident. The agency computer security incident response team shall convene upon notification of an information technology security incident and must comply with all applicable guidelines and processes established pursuant to paragraph (3)(c).

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

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

2. The state agency operational information technology security plan must include a progress report that objectively measures progress made towards the prior operational information technology security plan and a project plan that includes

activities, timelines, and deliverables for security objectives that the state agency will implement during the current fiscal year.

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

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

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

(h) Ensure that the information technology security and cybersecurity requirements in both the written specifications for the solicitation and service-level agreement of information technology and information technology resources and services meet or exceed the applicable state and federal laws, regulations, and standards for information technology security and cybersecurity. Service-level agreements must identify service provider and state agency responsibilities for privacy and security, protection of government data, personnel background screening, and security deliverables with associated frequencies.

(i) Provide information technology security and

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

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

1. All information technology security incidents and breaches must be reported to the Division of State Technology 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 information technology security breaches, state agencies shall provide notice in accordance with s. 501.171.

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

of:

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

(b)~~b.~~ Information technology resources, which includes:

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

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

~~Such records shall be available to the Auditor General, the Division of State Technology within the department, the Cybercrime Office of the Department of Law Enforcement, and, for state agencies under the jurisdiction of the Governor, the Chief Inspector General. Such records may be made available to a local government, another state agency, or a federal agency for information technology security purposes or in furtherance of the state agency's official duties. This exemption applies to such records held by a state agency before, on, or after the effective date of this exemption. This subparagraph is subject to the Open Government Sunset Review Act in accordance with s. 119.15 and shall stand repealed on October 2, 2021, unless reviewed and saved from repeal through reenactment by the Legislature.~~

(6)~~(5)~~ The portions of risk assessments, evaluations, external audits, and other reports of a state agency's information technology security program for the data, information, and information technology resources of the state

agency which are held by a state agency are confidential and exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution if the disclosure of such portions of records would facilitate unauthorized access to or the unauthorized modification, disclosure, or destruction of:

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

(b) Information technology resources, which include:

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

2. Security information, whether physical or virtual, which relates to the agency's existing or proposed information technology systems. For purposes of this subsection, the term "external audit" means an audit that is conducted by an entity other than the state agency that is the subject of the audit.

(7) Those portions of a public meeting as specified in s. 286.011 which would reveal records that are confidential and exempt under subsection (5) or subsection (6) 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.

(8) The ~~Such~~ 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 Division of State Technology 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 information technology security purposes or in furtherance of the state agency's official duties. ~~For purposes of this subsection, "external audit" means an audit that is conducted by an entity other than the state agency that is the subject of the audit.~~

(9) The exemptions contained in subsections (5), (6), and (7) apply ~~This exemption applies~~ to ~~such~~ records held by a state agency before, on, or after the effective date of this exemption.

(10) Subsections (5), (6), and (7) are ~~This subsection is~~ subject to the Open Government Sunset Review Act in accordance with s. 119.15 and shall stand repealed on October 2, 2025 ~~2021~~, unless reviewed and saved from repeal through reenactment by the Legislature.

(11) ~~(6)~~ The department shall adopt rules relating to information technology security and to administer this section.

Section 2. (1)(a) The Legislature finds it is a public necessity that the following data or information held by a state agency be made confidential and exempt from s. 119.07(1), Florida Statutes, and s. 24(a), Article I of the State

Constitution:

1. Portions of records held by a state agency which contain network schematics, hardware and software configurations, encryption, or which identify detection, investigation, or response practices for suspected or confirmed information technology security incidents, including suspected or confirmed breaches, if the disclosure of such records would facilitate unauthorized access to or the unauthorized modification, disclosure, or destruction of:

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

b. Information technology resources, which include:

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

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

2. Portions of risk assessments, evaluations, external audits, and other reports of a state agency's information technology security programs, 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:

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

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

(b) Such records must be made confidential and exempt from public records requirements for the following reasons:

1. Portions of records held by a state agency which contain network schematics, hardware and software configurations, encryption, or which identify information technology detection, investigation, or response practices for suspected or confirmed information technology security incidents or breaches are likely to be used in the investigations of the incidents or breaches. The release of such information could impede the investigation and impair the ability of reviewing entities to effectively and efficiently execute their investigative duties. In addition, the release of such information before an active investigation is completed could jeopardize the ongoing investigation.

2. An investigation of an information technology security incident or breach is likely to result in the gathering of sensitive personal information, including identification numbers and personal financial and health information. Such information could be used to commit identity theft or other crimes. In addition, release of such information could subject possible victims of the security incident or breach to further harm.

3. Disclosure of a record, including a computer forensic analysis, or other information that would reveal weaknesses in a state agency's data security could compromise that security in the future if such information were available upon conclusion of an investigation or once an investigation ceased to be active.

4. Such records are likely to contain proprietary

information about the security of the system at issue. The disclosure of such information could result in the identification of vulnerabilities and further breaches of that system. In addition, the release of such information could give business competitors an unfair advantage and weaken the security technology supplier supplying the proprietary information in the marketplace.

5. The disclosure of such records could potentially compromise the confidentiality, integrity, and availability of state agency data and information technology resources, which would significantly impair the administration of vital state programs. It is necessary that this information be made confidential in order to protect the technology systems, resources, and data of state agencies.

6. It is valuable, prudent, and critical to a state agency to have an independent entity conduct a risk assessment, an audit, or an evaluation or complete a report of the agency's information technology program or related systems. Such documents would likely include an analysis of the agency's current information technology program or systems which could clearly identify vulnerabilities or gaps in current systems or processes and propose recommendations to remedy identified vulnerabilities.

(2)(a)1. The Legislature also finds that it is a public necessity that those portions of a public meeting which would reveal data and information described in paragraph (1)(a) be made exempt from s. 286.011, Florida Statutes, and s. 24(b), Article I of the State Constitution.

2. Such meetings must be made exempt from open meetings

requirements in order to protect agency information technology systems, resources, and data. This information would clearly identify a state agency's information technology systems and its vulnerabilities and disclosure of such information would jeopardize the information technology security of the state agency and compromise the integrity and availability of state agency data and information technology resources. Such disclosure would significantly impair the administration of state programs.

(b)1. The Legislature further finds that it is a public necessity that the recordings and transcripts of the portions of meetings specified in subparagraph (a)1. be made confidential and exempt from s. 119.07(1), Florida Statutes, and s. 24(a), Article I of the State Constitution.

2. It is necessary that the resulting recordings and transcripts be made confidential and exempt from public record requirements in order to protect state information technology systems, resources, and data. The disclosure of such recordings and transcripts would clearly identify a state agency's information technology systems and its vulnerabilities. This disclosure would jeopardize the information technology security of the agency and compromise the integrity and availability of state data and information technology resources, which would significantly impair the administration of state programs.

(3) The Legislature further finds that these public meeting and public records exemptions must be given retroactive application because they are remedial in nature.

Section 3. This act shall take effect upon becoming a law.