CHAPTER 2025-27

Senate Bill No. 7020

An act relating to a review under the Open Government Sunset Review Act; amending s. 119.0725, F.S., which provides exemptions from public records requirements for agency cybersecurity information held by a state agency and exemptions from public meetings requirements for portions of meetings which would reveal confidential and exempt information; revising the date of the scheduled repeal of such exemptions; amending s. 282.318, F.S., which provides exemptions from public records and public meetings requirements for 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 that state agency which are held by a state agency and for portions of a public meeting which would reveal such confidential and exempt records; extending the date of the scheduled repeal of such exemptions; providing an effective date.

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

Section 1. Section 119.0725, Florida Statutes, is amended to read:

119.0725 Agency cybersecurity information; public records exemption; public meetings exemption.—

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

(a) "Breach" means unauthorized access of data in electronic form containing personal information. Good faith access of personal information by an employee or agent of an agency does not constitute a breach, provided that the information is not used for a purpose unrelated to the business or subject to further unauthorized use.

(b) "Critical infrastructure" means existing and proposed information technology and operational technology systems and assets, whether physical or virtual, the incapacity or destruction of which would negatively affect security, economic security, public health, or public safety.

(c) "Cybersecurity" has the same meaning as in s. 282.0041.

(d) "Data" has the same meaning as in s. 282.0041.

(e) "Incident" means a violation or imminent threat of violation, whether such violation is accidental or deliberate, of information technology resources, security, policies, or practices. As used in this paragraph, the term "imminent threat of violation" means a situation in which the agency has a factual basis for believing that a specific incident is about to occur.

(f) "Information technology" has the same meaning as in s. 282.0041.

(g) "Operational technology" means the hardware and software that cause or detect a change through the direct monitoring or control of physical devices, systems, processes, or events.

(2) The following information held by an agency is confidential and exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution:

(a) Coverage limits and deductible or self-insurance amounts of insurance or other risk mitigation coverages acquired for the protection of information technology systems, operational technology systems, or data of an agency.

(b) Information relating to critical infrastructure.

(c) Cybersecurity incident information reported pursuant to s. 282.318 or s. 282.3185.

(d) Network schematics, hardware and software configurations, or encryption information or information that identifies detection, investigation, or response practices for suspected or confirmed cybersecurity incidents, including suspected or confirmed breaches, if the disclosure of such information would facilitate unauthorized access to or unauthorized modification, disclosure, or destruction of:

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

2. Information technology resources, which include an agency's existing or proposed information technology systems.

(3) Any portion of a meeting that would reveal information made confidential and exempt under subsection (2) is exempt from s. 286.011 and s. 24(b), Art. I of the State Constitution. An exempt portion of a meeting may not be off the record and must be recorded and transcribed. The recording and transcript are confidential and exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution.

(4) The public records exemptions contained in this section apply to information held by an agency before, on, or after July 1, 2022.

(5)(a) Information made confidential and exempt pursuant to this section shall be made available to a law enforcement agency, the Auditor General, the Cybercrime Office of the Department of Law Enforcement, the Florida Digital Service within the Department of Management Services, and, for agencies under the jurisdiction of the Governor, the Chief Inspector General.

(b) Such confidential and exempt information may be disclosed by an agency in the furtherance of its official duties and responsibilities or to another agency or governmental entity in the furtherance of its statutory duties and responsibilities.

(6) Agencies may report information about cybersecurity incidents in the aggregate.

(7) This section is subject to the Open Government Sunset Review Act in accordance with s. 119.15 and shall stand repealed on October 2, 2026 ~~2027~~, unless reviewed and saved from repeal through reenactment by the Legislature.

Section 2. Subsection (9) of section 282.318, Florida Statutes, is amended, and subsections (5) and (6) of that section are republished, to read:

282.318 Cybersecurity.—

(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.

(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, 2026 ~~2025~~, unless reviewed and saved from repeal through reenactment by the Legislature.

Section 3. This act shall take effect July 1, 2025.

Approved by the Governor May 16, 2025.

Filed in Office Secretary of State May 16, 2025.