By the Committees on Appropriations; and Military and Veterans Affairs, Space, and Domestic Security; and Senator Hutson

576-03524-22 20221694c2

A bill to be entitled

An act relating to public records and public meetings; creating s. 119.0725, F.S.; providing definitions; providing an exemption from public records requirements for certain cybersecurity insurance information, critical infrastructure information, and certain cybersecurity-related information held by an agency; providing an exemption from public meetings requirements for portions of a meeting that would reveal certain cybersecurity-related information held by an agency; requiring the recording and transcription of exempt portions of such meetings; providing an exemption from public records requirements for such recordings and transcripts; providing retroactive application; authorizing the disclosure of confidential and exempt information under certain circumstances; authorizing agencies to report certain cybersecurity information in the aggregate; providing for future legislative review and repeal of the exemptions; amending ss. 98.015 and 282.318, F.S.; conforming provisions to changes made by the act; providing a statement of public necessity; providing a contingent effective date.

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

Section 1. Section 119.0725, Florida Statutes, is created 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) 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, 2027, unless reviewed and saved from repeal through reenactment by the Legislature.

Section 2. Subsection (13) of section 98.015, Florida Statutes, is amended to read:

98.015 Supervisor of elections; election, tenure of office, compensation, custody of registration-related documents, office hours, successor, seal; appointment of deputy supervisors; duties~~; public records exemption~~.—

~~(13)(a) Portions of records held by a supervisor of elections 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:~~

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

~~2. Information technology resources as defined in s. 119.011(9), which includes:~~

~~a. Information relating to the security of a supervisor of elections' technology, processes, and practices designed to protect networks, computers, data processing software, and data from attack, damage, or unauthorized access; or~~

~~b. Security information, whether physical or virtual, which relates to a supervisor of elections' existing or proposed information technology systems.~~

~~(b) The portions of records made confidential and exempt in paragraph (a) shall be available to the Auditor General and may be made available to another governmental entity for information technology security purposes or in the furtherance of the entity's official duties.~~

~~(c) The public record exemption in paragraph (a) applies to records held by a supervisor of elections before, on, or after the effective date of the exemption.~~

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

Section 3. Subsections (6) and (11) of section 282.318, Florida Statutes, are renumbered as subsections (5) and (10), respectively, and present subsections (5), (7), (8), (9), and (10) of that section are amended to read:

282.318 Cybersecurity.—

~~(5) 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 cybersecurity incidents, including suspected or confirmed breaches, are confidential and exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution, if the disclosure of such records would facilitate unauthorized access to or the unauthorized modification, disclosure, or destruction of:~~

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

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

~~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.~~

(6)~~(7)~~ Those portions of a public meeting as specified in s. 286.011 which would reveal records which 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.

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

(9) ~~(10)~~ Subsections (5) and~~,~~ (6)~~, and (7)~~ 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.

Section 4. (1) The Legislature finds that it is a public necessity that the following information held by an agency be made confidential and exempt from s. 119.07(1), Florida Statutes, and s. 24(a), Article 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) 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.

Release of such information could place an agency at greater risk of breaches, cybersecurity incidents, and ransomware attacks. Such information could be used by criminals to identify any vulnerabilities that may exist in an agency's security system, thereby compromising the integrity of the agency's information technology, operational technology, and data. If information related to the coverage limits and deductible or self-insurance amounts of cybersecurity insurance were disclosed, it could give cybercriminals an understanding of the monetary sum an agency can afford or may be willing to pay as a result of a ransomware attack at the expense of the taxpayer. In addition, critical infrastructure information is a vital component of public safety and, if made publicly available, could aid in the planning of, training for, and execution of cyberattacks, thereby increasing the ability of persons to harm individuals in this state. The recent cybersecurity hacking and shutdown of the Colonial Pipeline by the criminal enterprise

DarkSide in 2021 and the infiltration of the Bowman Avenue Dam in Rye Brook, New York, by Iranian hackers in 2013 provide evidence that such criminal capabilities exist. These events also show the crippling effect that cyberattacks on critical infrastructure may have. Further, the release of 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, would facilitate unauthorized access to or the unauthorized modification, disclosure, or destruction of data or information, whether physical or virtual, or information technology resources. Such information also includes proprietary information about the security of an agency's system. The disclosure of such information could compromise the integrity of an agency's data, information, or information technology resources, which would significantly impair the administration of vital governmental programs. Therefore, this information should be made confidential and exempt in order to protect the agency's data, information, and information technology resources.

(2) The Legislature also finds that it is a public necessity that any portion of a meeting that would reveal the confidential and exempt information be made exempt from s. 286.011, Florida Statutes, and s. 24(b), Article I of the State Constitution, and that any recordings and transcripts of the closed portion of a meeting be made confidential and exempt from s. 119.07(1), Florida Statutes, and s. 24(a), Article I of the State Constitution. The failure to close that portion of a

meeting at which confidential and exempt information would be revealed, and prevent the disclosure of the recordings and transcripts of those portions of a meeting, would defeat the purpose of the underlying public records exemption and could result in the release of highly sensitive information related to the cybersecurity of an agency system.

(3) For these reasons, the Legislature finds that these public records and public meetings exemptions are of the utmost importance and are a public necessity.

Section 5. This act shall take effect on the same date that SB 1670 or similar legislation takes effect, if such legislation is adopted in the same legislative session or an extension thereof and becomes law.