A bill to be entitled

An act relating to public records and public meetings; amending s. 119.0713, F.S.; providing definitions; providing an exemption from public records requirements for certain insurance records and critical energy infrastructure information held by a local government; providing an exemption from public records requirements for certain records held by a local government 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; providing an exemption from public meetings requirements for portions of public meetings which would reveal such information; providing an exemption from public records requirements for the recording and transcript of such meetings; providing exceptions; providing for future legislative review and repeal of the exemptions; providing a statement of public necessity; providing an effective date.

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

Section 1. Subsection (6) is added to section 119.0713,

Florida Statutes, to read:

119.0713 Local government agency exemptions from inspection or copying of public records.—

(6)(a) As used in this subsection, the term:

1. "Critical energy infrastructure information" means specific engineering, vulnerability, or detailed design information about proposed or existing critical infrastructure which:

a. Includes details about the production, generation, transportation, transmission, or distribution of energy.

b. May be useful in planning an attack on critical infrastructure.

c. Provides more detailed location information than the general location of the critical infrastructure.

2. "Critical infrastructure" means existing and proposed systems and assets, whether physical or virtual, the incapacity or destruction of which would negatively affect security, economic security, public health, or public safety, including information technology and operation technology systems and data of a local government.

3. "Local government" means a county, municipality, special district, local agency, authority, consolidated city-county government, or any other local governmental body or public body corporate or politic authorized or created by general or special law.

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

1. Information related to insurance or other risk mitigation products or coverages, including deductible or self-insurance amounts, coverage limits, and policy terms and conditions, for the protection of the information technology and operational technology systems and data of a local government.

2. Critical energy infrastructure information.

3. Any portion of a record that contains network schematics, hardware and software configurations, or encryption or that identifies detection, investigation, or response practices for suspected or confirmed cybersecurity incidents, including suspected or confirmed breaches, if the disclosure of such record 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, including:

(I) Information relating to the security of the local government'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 local government's existing or proposed information technology systems.

(c) Any portion of a meeting that would reveal information made confidential and exempt under paragraph (b) is exempt from s. 286.011 and s. 24(b), Art. I of the State Constitution. No exempt portion of a meeting may be off the record. All exempt portions of such a meeting must be recorded and transcribed. The recording and transcript of the meeting are confidential and exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution unless a court of competent jurisdiction, following an in camera review, determines that the meeting was not restricted to the discussion of information made confidential and exempt by this subsection. In the event of such a judicial determination, only that portion of the transcript that reveals nonexempt information may be disclosed.

(d) Information made confidential and exempt under this subsection must be made available to law enforcement agencies, the Auditor General, the Cybercrime Office of the Department of Law Enforcement, and the Florida Digital Service. Such information may be made available to another governmental entity for security purposes or in furtherance of such entity's official duties.

(e) This subsection 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. (1) The Legislature finds that it is a public

necessity that information held by a local government and related to insurance coverage amounts, premium amount paid, self-insurance amounts, and policy terms and conditions of such cybersecurity insurance policies; and critical energy infrastructure information created or received by the local government which consists of details about the production, generation, transportation, transmission, or distribution of energy be made confidential and exempt from s. 119.07(1), Florida Statutes, and s. 24(a), Article I of the State Constitution. Such information held by a local government is critical information, the release of which could lead to extreme danger or harm to the citizens of the state. Typical critical energy infrastructure information held by a local government consists of critical asset location, vulnerable electric grid transmission information, emerging technologies utilized by the local government to prevent a cyberattack, and secure information that local governments in the state share with regional and federal entities. The exposure or leak of such information could lead to interruptions in the delivery of essential services, as well as financial or physical harm to the citizens of the state. Critical energy infrastructure information has been defined and codified in law in over half of the states in the United States in conjunction with the Federal Energy Regulatory Commission. Local governments in the state have recently been attacked by criminals who hold hostage

critical data and operability of the local government for ransom. Public disclosure of insurance coverages provides information to potential attackers as to the monetary limits to which they may seek ransom from these local governments. These vulnerabilities leave all local governments throughout the state exposed to cyberattacks and ransom demands. The Legislature finds that the harm that may result from the release of such information outweighs any public benefit that may be derived from disclosure of the information.

(2)(a) The Legislature finds that it is a public necessity that the following information be made confidential and exempt from s. 119.07(1), Florida Statutes, and s. 24(a), Article I of the State Constitution:

1. Records held by a local government 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 unauthorized modification, disclosure, or destruction of:

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

b. Information technology resources, including:

(I) Information relating to the security of the local government'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 local government's existing or proposed information technology systems.

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

1. Records held by a local government 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. 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 local government'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 local government data and information technology resources, which would significantly impair the administration of vital governmental programs. It is necessary that this information be made confidential in order to protect the technology systems, resources, and data of local governments. The Legislature further finds that this public records exemption be given retroactive application because it is remedial in nature.

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

remain confidential and exempt from disclosure under s. 119.07(1), Florida Statutes, and s. 24(a), Article I of the State Constitution unless a court of competent jurisdiction, following an in camera review, determines that the meeting was not restricted to the discussion of data and information made confidential and exempt by this act. In the event of such a judicial determination, only that portion of the transcript which reveals nonexempt data and information may be disclosed to a third party. It is necessary that such meetings be made exempt from public meetings requirements in order to protect local government information technology systems, resources, and data. The information disclosed during portions of meetings would clearly identify a local government's information technology systems and its vulnerabilities. This disclosure would jeopardize the information technology security of the local government and compromise the integrity and availability of local government data and information technology resources, which would significantly impair the administration of government programs.

2. The Legislature further finds that it is a public necessity that the recording and transcript of those portions of meetings specified in subparagraph 1. be made confidential and exempt from s. 119.07(1), Florida Statutes, and s. 24(a), Article I of the State Constitution unless a court determines that the meeting was not restricted to the discussion of

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

Section 3. This act shall take effect July 1, 2022.