CHAPTER 2018-65

Committee Substitute for
Committee Substitute for House Bill No. 1127

An act relating to public records and public meetings; creating s. 627.352, F.S.; providing an exemption from public records requirements for certain records held by the Citizens Property Insurance Corporation which identify detection, investigation, or response practices for suspected or confirmed information technology security incidents; creating an exemption from public records requirements for certain portions of risk assessments, evaluations, audits, and other reports of the corporation's information technology security program; creating an exemption from public meetings requirements for portions of public meetings which would reveal such data and information; providing an exemption from public records requirements for a specified period for the recording and transcript of a closed meeting; authorizing disclosure of confidential and exempt information to certain agencies and officers; providing for future legislative review and repeal; providing a statement of public necessity; providing retroactive application; providing an effective date.

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

Section 1. Section 627.352, Florida Statutes, is created to read:

627.352 Security of data and information technology in Citizens Property Insurance Corporation.—

(1) The following data and information from technology systems owned by, under contract with, or maintained by Citizens Property Insurance Corporation are confidential and exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution:

(a) Records held by the corporation 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:

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

2. Information technology resources, including:

a. Information relating to the security of the corporation's technologies, 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 the corporation's existing or proposed information technology systems.

(b) Those portions of risk assessments, evaluations, audits, and other reports of the corporation's information technology security program for its data, information, and information technology resources which are held by the corporation, 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, which include:

a. Information relating to the security of the corporation's technologies, 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 the corporation's existing or proposed information technology systems.

(2) Those portions of a public meeting as specified in s. 286.011 which would reveal data and information described in subsection (1) 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 a meeting must be recorded and transcribed. The recording and transcript of the meeting must remain confidential and exempt from disclosure under s. 119.07(1) and s. 24(a), Art. 1 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 section. 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.

(3) The records and portions of public meeting recordings and transcripts described in subsection (2) must be available to the Auditor General, the Cybercrime Office of the Department of Law Enforcement, and the Office of Insurance Regulation. Such records and portions of meetings, recordings, and transcripts may be made available to a state or federal agency for security purposes or in furtherance of the agency's official duties.

(4) The exemptions provided by this section apply to records held by the corporation before, on, or after the effective date of this act.

(5) This section is subject to the Open Government Sunset Review Act in accordance with s. 119.15 and shall stand repealed on October 2, 2023, unless reviewed and saved from repeal through reenactment by the Legislature.

Section 2. (1)(a) The Legislature finds that it is a public necessity that the following data or information from technology systems owned, under contract, or maintained by the corporation be confidential and exempt from s. 119.07 (1), Florida Statutes, and s. 24 (a), Article I of the State Constitution:

1. Records held by the corporation 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, which include:

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

2. Those portions of risk assessments, evaluations, audits, and other reports of the corporation's information technology security program for its data, information, and information technology resources which are held by the corporation, 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 corporation'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 corporation's existing or proposed information technology systems.

(b) The Legislature also finds that those portions of a public meeting as specified in s. 286.011, Florida Statutes, which would reveal data and information described in subsection (1) are 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 section. 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.

(c) The Legislature further finds that it is a public necessity that records held by the corporation which identify detection, investigation, or response

practices for suspected or confirmed information technology security incidents, including suspected or confirmed breaches, be made confidential and exempt from s. 119.07 (1), Florida Statutes, and s. 24 (a), Article 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, which include:

a. Information relating to the security of the corporation's technologies, 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 the corporation's existing or proposed information technology systems.

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

1. Records held by the corporation 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 the corporation'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 the corporation's data and information technology resources. It is a public necessity that this information be made confidential in order to protect the technology systems, resources, and data of the corporation. The Legislature further finds that this public records exemption be given retroactive application because it is remedial in nature.

(2)(a) The Legislature also finds that it is a public necessity that portions of risk assessments, evaluations, audits, and other reports of the corporation's information technology security program for its data, information, and information technology resources which are held by the corporation be made confidential and exempt from s. 119.07 (1), Florida Statutes, and s. 24 (a), Article 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:

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

2. Information technology resources, which include:

a. Information relating to the security of the corporation's technologies, 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 the corporation's existing or proposed information technology systems.

(b) The Legislature finds that it is valuable, prudent, and critical to the corporation to have an independent entity conduct a risk assessment, an audit, or an evaluation or complete a report of the corporation's information technology program or related systems. Such documents would likely include an analysis of the corporation'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.

(3)(a) The Legislature further finds that it is a public necessity that those portions of a public meeting which could reveal information described in this section be made exempt from s. 286.011, Florida Statutes, and s. 24 (b), Article I of the State Constitution. It is a public necessity that such meetings be made exempt from the open meetings requirements in order to protect the corporation's information technology systems, resources, and data. The information disclosed during portions of meetings would clearly identify the corporation's information technology systems and its vulnerabilities. This disclosure would jeopardize the information technology security of the corporation and compromise the integrity and availability of the corporation's data and information technology resources.

(b) The Legislature further finds that it is a public necessity that the recording and transcript of those portions of meetings specified in paragraph (a) 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 data and information made confidential and exempt by this act. It is a public necessity that the resulting recordings and transcripts be made confidential and exempt from the public records requirements in order to protect the corporation's information technology systems, resources, and data. The disclosure of such recordings and transcripts would clearly identify the corporation's information technology systems and its vulnerabilities. This disclosure would jeopardize the information technology security of the corporation and compromise the integrity and availability of the corporation's data and information technology resources.

(c) The Legislature further finds that this public records exemption must be given retroactive application because it is remedial in nature.

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

Approved by the Governor March 21, 2018.

Filed in Office Secretary of State March 21, 2018.