CHAPTER 2016-114

Committee Substitute for Senate Bill No. 624

An act relating to public records; amending s. 282.318, F.S.; creating exemptions from public records requirements for certain records held by a state agency which identify detection, investigation, or response practices for suspected or confirmed information technology security incidents and for certain portions of risk assessments, evaluations, external audits, and other reports of a state agency's information technology program; authorizing disclosure of confidential and exempt information to certain agencies and officers; providing for retroactive application; providing for future legislative review and repeal 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. Paragraph (i) of subsection (4) of section 282.318, Florida Statutes, is amended, present subsection (5) of that section is renumbered as subsection (6), and a new subsection (5) is added to that section, to read:

282.318 Security of data and information technology.—

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

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

1. All information technology security incidents and breaches must be reported to the Agency for State Technology.

2. For information technology security breaches, state agencies shall provide notice in accordance with s. 501.171.

3. Records held by a state agency 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. Data or information, whether physical or virtual; or

b. Information technology resources, which includes:

(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.

Such records shall be available to the Auditor General, the Agency for State Technology, 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.

(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.

Such portions of records shall be available to the Auditor General, the Cybercrime Office of the Department of Law Enforcement, the Agency for State Technology, 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. This exemption applies to such records held by a state agency before, on, or after the effective date of this exemption. This subsection 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.

Section 2. (1)(a) The Legislature finds that it is a public necessity that public records held by a state agency 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 includes:

a. 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

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

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

1. Records held by a state agency which identify information technology detection, investigation, or response practices for suspected or confirmed information technology incidents or breaches are likely to be used in the investigation of the incident or breach. 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 completion of an active investigation 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 not otherwise exempt or confidential and exempt from public records requirements under any other law. Such information could be used for the purpose of identity theft or other crimes. In addition, release of such information could subject possible victims of the 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 the future security of that agency or other entities if such information were available upon conclusion of an investigation or once an investigation ceased to be active. The disclosure of such a record or

information could compromise the security of state agencies and make those state agencies susceptible to future data incidents or breaches.

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 position of the entity 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 governmental programs. It is necessary that this information be made confidential in order to protect the technology systems, resources, and data of state agencies. 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, 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 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 includes:

a. 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

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

(b) The Legislature finds that it may be valuable, prudent, or 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 state agency's information technology program or related systems. Such documents would likely include an analysis of the state 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. The disclosure of such portions of records would jeopardize the information technology security of the state agency, and compromise the integrity and availability of agency data and information

technology resources, which would significantly impair the administration of governmental programs. It is necessary that such portions of records be made confidential and exempt from public records requirements in order to protect agency technology systems, resources, and data. The Legislature further finds that this public records exemption shall 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 25, 2016.

Filed in Office Secretary of State March 25, 2016.