

1 A bill to be entitled
 2 An act relating to public records; amending s.
 3 282.318, F.S.; creating exemptions from public records
 4 requirements for certain records held by a state
 5 agency which identify detection, investigation, or
 6 response practices for suspected or confirmed
 7 information technology security incidents and for
 8 certain portions of risk assessments, evaluations,
 9 external audits, and other reports of a state agency's
 10 information technology program; authorizing disclosure
 11 of confidential and exempt information to certain
 12 agencies and officers; providing for retroactive
 13 application; providing for future legislative review
 14 and repeal of the exemptions; providing statements of
 15 public necessity; providing a contingent effective
 16 date.

17
 18 Be It Enacted by the Legislature of the State of Florida:
 19
 20

21 Section 1. Paragraph (i) of subsection (4) of section
 22 282.318, Florida Statutes, is amended, present subsection (5) of
 23 that section is renumbered as subsection (6), and a new
 24 subsection (5) is added to that section, to read:

25 282.318 Security of data and information technology.—
 26 (4) Each state agency head shall, at a minimum:

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

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

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

36 3. Records held by a state agency which identify
 37 detection, investigation, or response practices for suspected or
 38 confirmed information technology security incidents, including
 39 suspected or confirmed breaches, are confidential and exempt
 40 from s. 119.07(1) and s. 24(a), Art. I of the State
 41 Constitution, if the disclosure of such records would facilitate
 42 unauthorized access to or the unauthorized modification,
 43 disclosure, or destruction of:

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

45 b. Information technology resources, which includes:

46 (I) Information relating to the security of the agency's
 47 technologies, processes, and practices designed to protect
 48 networks, computers, data processing software, and data from
 49 attack, damage, or unauthorized access; or

50 (II) Security information, whether physical or virtual,
 51 which relates to the agency's existing or proposed information
 52 technology systems.

53
 54 Such records shall be available to the Auditor General, the
 55 Agency for State Technology, the Cybercrime Office of the
 56 Department of Law Enforcement, and, for state agencies under the
 57 jurisdiction of the Governor, the Chief Inspector General. Such
 58 records may be made available to a local government, another
 59 state agency, or a federal agency for information technology
 60 security purposes or in furtherance of the state agency's
 61 official duties. This exemption applies to such records held by
 62 a state agency before, on, or after the effective date of this
 63 exemption. This subparagraph is subject to the Open Government
 64 Sunset Review Act in accordance with s. 119.15 and shall stand
 65 repealed on October 2, 2021, unless reviewed and saved from
 66 repeal through reenactment by the Legislature.

67 (5) The portions of risk assessments, evaluations,
 68 external audits, and other reports of a state agency's
 69 information technology security program for the data,
 70 information, and information technology resources of the state
 71 agency which are held by a state agency are confidential and
 72 exempt from s. 119.07(1) and s. 24(a), Art. I of the State
 73 Constitution if the disclosure of such portions of records would
 74 facilitate unauthorized access to or the unauthorized
 75 modification, disclosure, or destruction of:

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

77 (b) Information technology resources, which include:

78 1. Information relating to the security of the agency's

79 technologies, processes, and practices designed to protect
 80 networks, computers, data processing software, and data from
 81 attack, damage, or unauthorized access; or

82 2. Security information, whether physical or virtual,
 83 which relates to the agency's existing or proposed information
 84 technology systems.

85
 86 Such portions of records shall be available to the Auditor
 87 General, the Cybercrime Office of the Department of Law
 88 Enforcement, the Agency for State Technology, and, for agencies
 89 under the jurisdiction of the Governor, the Chief Inspector
 90 General. Such portions of records may be made available to a
 91 local government, another state agency, or a federal agency for
 92 information technology security purposes or in furtherance of
 93 the state agency's official duties. For purposes of this
 94 subsection, "external audit" means an audit that is conducted by
 95 an entity other than the state agency that is the subject of the
 96 audit. This exemption applies to such records held by a state
 97 agency before, on, or after the effective date of this
 98 exemption. This subsection is subject to the Open Government
 99 Sunset Review Act in accordance with s. 119.15 and shall stand
 100 repealed on October 2, 2021, unless reviewed and saved from
 101 repeal through reenactment by the Legislature.

102 Section 2. (1)(a) The Legislature finds that it is a
 103 public necessity that public records held by a state agency
 104 which identify detection, investigation, or response practices

105 for suspected or confirmed information technology security
106 incidents, including suspected or confirmed breaches, be made
107 confidential and exempt from s. 119.07(1), Florida Statutes, and
108 s. 24(a), Article I of the State Constitution if the disclosure
109 of such records would facilitate unauthorized access to or the
110 unauthorized modification, disclosure, or destruction of:

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

112 2. Information technology resources, which includes:

113 a. Information relating to the security of the agency's
114 technologies, processes, and practices designed to protect
115 networks, computers, data processing software, and data from
116 attack, damage, or unauthorized access; or

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

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

122 1. Records held by a state agency which identify
123 information technology detection, investigation, or response
124 practices for suspected or confirmed information technology
125 incidents or breaches are likely to be used in the investigation
126 of the incident or breach. The release of such information could
127 impede the investigation and impair the ability of reviewing
128 entities to effectively and efficiently execute their
129 investigative duties. In addition, the release of such
130 information before completion of an active investigation could

131 jeopardize the ongoing investigation.

132 2. An investigation of an information technology security
133 incident or breach is likely to result in the gathering of
134 sensitive personal information, including identification numbers
135 and personal financial and health information not otherwise
136 exempt or confidential and exempt from public records
137 requirements under any other law. Such information could be used
138 for the purpose of identity theft or other crimes. In addition,
139 release of such information could subject possible victims of
140 the incident or breach to further harm.

141 3. Disclosure of a record, including a computer forensic
142 analysis, or other information that would reveal weaknesses in a
143 state agency's data security could compromise the future
144 security of that agency or other entities if such information
145 were available upon conclusion of an investigation or once an
146 investigation ceased to be active. The disclosure of such a
147 record or information could compromise the security of state
148 agencies and make those state agencies susceptible to future
149 data incidents or breaches.

150 4. Such records are likely to contain proprietary
151 information about the security of the system at issue. The
152 disclosure of such information could result in the
153 identification of vulnerabilities and further breaches of that
154 system. In addition, the release of such information could give
155 business competitors an unfair advantage and weaken the position
156 of the entity supplying the proprietary information in the

157 marketplace.

158 5. The disclosure of such records could potentially
 159 compromise the confidentiality, integrity, and availability of
 160 state agency data and information technology resources, which
 161 would significantly impair the administration of vital
 162 governmental programs. It is necessary that this information be
 163 made confidential in order to protect the technology systems,
 164 resources, and data of state agencies. The Legislature further
 165 finds that this public records exemption be given retroactive
 166 application because it is remedial in nature.

167 (2)(a) The Legislature also finds that it is a public
 168 necessity that portions of risk assessments, evaluations,
 169 external audits, and other reports of a state agency's
 170 information technology security program for the data,
 171 information, and information technology resources of the state
 172 agency which are held by a state agency be made confidential and
 173 exempt from s. 119.07(1), Florida Statutes, and s. 24(a),
 174 Article I of the State Constitution if the disclosure of such
 175 portions of records would facilitate unauthorized access to or
 176 the unauthorized modification, disclosure, or destruction of:

- 177 1. Data or information, whether physical or virtual; or
- 178 2. Information technology resources, which includes:
 - 179 a. Information relating to the security of the agency's
 180 technologies, processes, and practices designed to protect
 181 networks, computers, data processing software, and data from
 182 attack, damage, or unauthorized access; or

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

186 (b) The Legislature finds that it may be valuable,
187 prudent, or critical to a state agency to have an independent
188 entity conduct a risk assessment, an audit, or an evaluation or
189 complete a report of the state agency's information technology
190 program or related systems. Such documents would likely include
191 an analysis of the state agency's current information technology
192 program or systems which could clearly identify vulnerabilities
193 or gaps in current systems or processes and propose
194 recommendations to remedy identified vulnerabilities. The
195 disclosure of such portions of records would jeopardize the
196 information technology security of the state agency, and
197 compromise the integrity and availability of agency data and
198 information technology resources, which would significantly
199 impair the administration of governmental programs. It is
200 necessary that such portions of records be made confidential and
201 exempt from public records requirements in order to protect
202 agency technology systems, resources, and data. The Legislature
203 further finds that this public records exemption shall be given
204 retroactive application because it is remedial in nature.

205 Section 3. This act shall take effect upon becoming a law,
206 if CS/CS/CS/HB 1033 or similar legislation is adopted in the
207 same legislative session or an extension thereof and becomes
208 law.