



272518

LEGISLATIVE ACTION

Senate	.	House
Comm: RCS	.	
03/02/2022	.	
	.	
	.	
	.	

The Committee on Appropriations (Hutson) recommended the following:

Senate Amendment (with title amendment)

Delete everything after the enacting clause and insert:

Section 1. Present subsections (28) through (37) of section 282.0041, Florida Statutes, are redesignated as subsections (29) through (38), respectively, a new subsection (28) is added to that section, and subsection (19) of that section is amended, to read:

282.0041 Definitions.—As used in this chapter, the term:



272518

11 (19) "Incident" means a violation or imminent threat of
12 violation, whether such violation is accidental or deliberate,
13 of information technology resources, security, policies, or
14 practices. An imminent threat of violation refers to a situation
15 in which a the state agency, county, or municipality has a
16 factual basis for believing that a specific incident is about to
17 occur.

18 (28) "Ransomware incident" means a malicious cybersecurity
19 incident in which a person or entity introduces software that
20 gains unauthorized access to or encrypts, modifies, or otherwise
21 renders unavailable a state agency's, county's, or
22 municipality's data and thereafter the person or entity demands
23 a ransom to prevent the publication of the data, restore access
24 to the data, or otherwise remediate the impact of the software.

25 Section 2. Paragraphs (c) and (g) of subsection (3) and
26 paragraphs (i) and (j) of subsection (4) of section 282.318,
27 Florida Statutes, are amended, and paragraph (k) is added to
28 subsection (4) of that section, to read:

29 282.318 Cybersecurity.—

30 (3) The department, acting through the Florida Digital
31 Service, is the lead entity responsible for establishing
32 standards and processes for assessing state agency cybersecurity
33 risks and determining appropriate security measures. Such
34 standards and processes must be consistent with generally
35 accepted technology best practices, including the National
36 Institute for Standards and Technology Cybersecurity Framework,
37 for cybersecurity. The department, acting through the Florida
38 Digital Service, shall adopt rules that mitigate risks;
39 safeguard state agency digital assets, data, information, and



40 information technology resources to ensure availability,
41 confidentiality, and integrity; and support a security
42 governance framework. The department, acting through the Florida
43 Digital Service, shall also:

44 (c) Develop and publish for use by state agencies a
45 cybersecurity governance framework that, at a minimum, includes
46 guidelines and processes for:

47 1. Establishing asset management procedures to ensure that
48 an agency's information technology resources are identified and
49 managed consistent with their relative importance to the
50 agency's business objectives.

51 2. Using a standard risk assessment methodology that
52 includes the identification of an agency's priorities,
53 constraints, risk tolerances, and assumptions necessary to
54 support operational risk decisions.

55 3. Completing comprehensive risk assessments and
56 cybersecurity audits, which may be completed by a private sector
57 vendor, and submitting completed assessments and audits to the
58 department.

59 4. Identifying protection procedures to manage the
60 protection of an agency's information, data, and information
61 technology resources.

62 5. Establishing procedures for accessing information and
63 data to ensure the confidentiality, integrity, and availability
64 of such information and data.

65 6. Detecting threats through proactive monitoring of
66 events, continuous security monitoring, and defined detection
67 processes.

68 7. Establishing agency cybersecurity incident response



69 teams and describing their responsibilities for responding to
70 cybersecurity incidents, including breaches of personal
71 information containing confidential or exempt data.

72 8. Recovering information and data in response to a
73 cybersecurity incident. The recovery may include recommended
74 improvements to the agency processes, policies, or guidelines.

75 9. Establishing a cybersecurity incident reporting process
76 that includes procedures ~~and tiered reporting timeframes~~ for
77 notifying the department and the Department of Law Enforcement
78 of cybersecurity incidents. ~~The tiered reporting timeframes~~
79 ~~shall be based upon the level of severity of the cybersecurity~~
80 ~~incidents being reported.~~

81 a. The level of severity of the cybersecurity incident is
82 defined by the National Cyber Incident Response Plan of the
83 United States Department of Homeland Security as follows:

84 (I) Level 5 is an emergency-level incident within the
85 specified jurisdiction that poses an imminent threat to the
86 provision of wide-scale critical infrastructure services;
87 national, state, or local government security; or the lives of
88 the country's, state's, or local government's residents.

89 (II) Level 4 is a severe-level incident that is likely to
90 result in a significant impact in the affected jurisdiction to
91 public health or safety; national, state, or local security;
92 economic security; or civil liberties.

93 (III) Level 3 is a high-level incident that is likely to
94 result in a demonstrable impact in the affected jurisdiction to
95 public health or safety; national, state, or local security;
96 economic security; civil liberties; or public confidence.

97 (IV) Level 2 is a medium-level incident that may impact



98 public health or safety; national, state, or local security;
99 economic security; civil liberties; or public confidence.

100 (V) Level 1 is a low-level incident that is unlikely to
101 impact public health or safety; national, state, or local
102 security; economic security; civil liberties; or public
103 confidence.

104 b. The cybersecurity incident reporting process must
105 specify the information that must be reported by a state agency
106 following a cybersecurity incident or ransomware incident,
107 which, at a minimum, must include the following:

108 (I) A summary of the facts surrounding the cybersecurity
109 incident or ransomware incident.

110 (II) The date on which the state agency most recently
111 backed up its data, the physical location of the backup, if the
112 backup was affected, and if the backup was created using cloud
113 computing.

114 (III) The types of data compromised by the cybersecurity
115 incident or ransomware incident.

116 (IV) The estimated fiscal impact of the cybersecurity
117 incident or ransomware incident.

118 (V) In the case of a ransomware incident, the details of
119 the ransom demanded.

120 c.(I) A state agency shall report all ransomware incidents
121 and any cybersecurity incident determined by the state agency to
122 be of severity level 3, 4, or 5 to the Cybersecurity Operations
123 Center and the Cybercrime Office of the Department of Law
124 Enforcement as soon as possible but no later than 48 hours after
125 discovery of the cybersecurity incident and no later than 12
126 hours after discovery of the ransomware incident. The report



127 must contain the information required in sub-subparagraph b.

128 (II) The Cybersecurity Operations Center shall notify the
129 President of the Senate and the Speaker of the House of
130 Representatives of any severity level 3, 4, or 5 incident as
131 soon as possible but no later than 12 hours after receiving a
132 state agency's incident report. The notification must include a
133 high-level description of the incident and the likely effects.

134 d. A state agency shall report a cybersecurity incident
135 determined by the state agency to be of severity level 1 or 2 to
136 the Cybersecurity Operations Center and the Cybercrime Office of
137 the Department of Law Enforcement as soon as possible. The
138 report must contain the information required in sub-subparagraph
139 b.

140 e. The Cybersecurity Operations Center shall provide a
141 consolidated incident report on a quarterly basis to the
142 President of the Senate, the Speaker of the House of
143 Representatives, and the Florida Cybersecurity Advisory Council.
144 The report provided to the Florida Cybersecurity Advisory
145 Council may not contain the name of any agency, network
146 information, or system identifying information but must contain
147 sufficient relevant information to allow the Florida
148 Cybersecurity Advisory Council to fulfill its responsibilities
149 as required in s. 282.319(9).

150 10. Incorporating information obtained through detection
151 and response activities into the agency's cybersecurity incident
152 response plans.

153 11. Developing agency strategic and operational
154 cybersecurity plans required pursuant to this section.

155 12. Establishing the managerial, operational, and technical



272518

156 safeguards for protecting state government data and information
157 technology resources that align with the state agency risk
158 management strategy and that protect the confidentiality,
159 integrity, and availability of information and data.

160 13. Establishing procedures for procuring information
161 technology commodities and services that require the commodity
162 or service to meet the National Institute of Standards and
163 Technology Cybersecurity Framework.

164 14. Submitting after-action reports following a
165 cybersecurity incident or ransomware incident. Such guidelines
166 and processes for submitting after-action reports must be
167 developed and published by December 1, 2022.

168 (g) Annually provide cybersecurity training to all state
169 agency technology professionals and employees with access to
170 highly sensitive information which ~~that~~ develops, assesses, and
171 documents competencies by role and skill level. The
172 cybersecurity training curriculum must include training on the
173 identification of each cybersecurity incident severity level
174 referenced in sub-subparagraph (c)9.a. The training may be
175 provided in collaboration with the Cybercrime Office of the
176 Department of Law Enforcement, a private sector entity, or an
177 institution of the State University System.

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

179 (i) Provide cybersecurity awareness training to all state
180 agency employees within in the first 30 days after commencing
181 employment, and annually thereafter, concerning cybersecurity
182 risks and the responsibility of employees to comply with
183 policies, standards, guidelines, and operating procedures
184 adopted by the state agency to reduce those risks. The training



185 may be provided in collaboration with the Cybercrime Office of
186 the Department of Law Enforcement, a private sector entity, or
187 an institution of the State University System.

188 (j) Develop a process for detecting, reporting, and
189 responding to threats, breaches, or cybersecurity incidents
190 which is consistent with the security rules, guidelines, and
191 processes established by the department through the Florida
192 Digital Service.

193 1. All cybersecurity incidents and ransomware incidents
194 ~~breaches~~ must be reported by state agencies. Such reports ~~to the~~
195 ~~Florida Digital Service within the department and the Cybercrime~~
196 ~~Office of the Department of Law Enforcement and~~ must comply with
197 the notification procedures and reporting timeframes established
198 pursuant to paragraph (3) (c).

199 2. For cybersecurity breaches, state agencies shall provide
200 notice in accordance with s. 501.171.

201 (k) Submit to the Florida Digital Service, within 1 week
202 after the remediation of a cybersecurity incident or ransomware
203 incident, an after-action report that summarizes the incident,
204 the incident's resolution, and any insights gained as a result
205 of the incident.

206 Section 3. Section 282.3185, Florida Statutes, is created
207 to read:

208 282.3185 Local government cybersecurity.-

209 (1) SHORT TITLE.-This section may be cited as the "Local
210 Government Cybersecurity Act."

211 (2) DEFINITION.-As used in this section, the term "local
212 government" means any county or municipality.

213 (3) CYBERSECURITY TRAINING.-



272518

214 (a) The Florida Digital Service shall:
215 1. Develop a basic cybersecurity training curriculum for
216 local government employees. All local government employees with
217 access to the local government's network must complete the basic
218 cybersecurity training within 30 days after commencing
219 employment and annually thereafter.
220 2. Develop an advanced cybersecurity training curriculum
221 for local governments which is consistent with the cybersecurity
222 training required under s. 282.318(3)(g). All local government
223 technology professionals and employees with access to highly
224 sensitive information must complete the advanced cybersecurity
225 training within 30 days after commencing employment and annually
226 thereafter.
227 (b) The Florida Digital Service may provide the
228 cybersecurity training required by this subsection in
229 collaboration with the Cybercrime Office of the Department of
230 Law Enforcement, a private sector entity, or an institution of
231 the State University System.
232 (4) CYBERSECURITY STANDARDS.—
233 (a) Each local government shall adopt cybersecurity
234 standards that safeguard its data, information technology, and
235 information technology resources to ensure availability,
236 confidentiality, and integrity. The cybersecurity standards must
237 be consistent with generally accepted best practices for
238 cybersecurity, including the National Institute of Standards and
239 Technology Cybersecurity Framework.
240 (b) Each county with a population of 75,000 or more must
241 adopt the cybersecurity standards required by this subsection by
242 January 1, 2024. Each county with a population of less than



243 75,000 must adopt the cybersecurity standards required by this
244 subsection by January 1, 2025.

245 (c) Each municipality with a population of 25,000 or more
246 must adopt the cybersecurity standards required by this
247 subsection by January 1, 2024. Each municipality with a
248 population of less than 25,000 must adopt the cybersecurity
249 standards required by this subsection by January 1, 2025.

250 (d) Each local government shall notify the Florida Digital
251 Service of its compliance with this subsection as soon as
252 possible.

253 (5) INCIDENT NOTIFICATION.—

254 (a) A local government shall provide notification of a
255 cybersecurity incident or ransomware incident to the
256 Cybersecurity Operations Center, Cybercrime Office of the
257 Department of Law Enforcement, and sheriff who has jurisdiction
258 over the local government in accordance with paragraph (b). The
259 notification must include, at a minimum, the following
260 information:

261 1. A summary of the facts surrounding the cybersecurity
262 incident or ransomware incident.

263 2. The date on which the local government most recently
264 backed up its data, the physical location of the backup, if the
265 backup was affected, and if the backup was created using cloud
266 computing.

267 3. The types of data compromised by the cybersecurity
268 incident or ransomware incident.

269 4. The estimated fiscal impact of the cybersecurity
270 incident or ransomware incident.

271 5. In the case of a ransomware incident, the details of the



272518

272 ransom demanded.

273 6. A statement requesting or declining assistance from the
274 Cybersecurity Operations Center, the Cybercrime Office of the
275 Department of Law Enforcement, or the sheriff who has
276 jurisdiction over the local government.

277 (b)1. A local government shall report all ransomware
278 incidents and any cybersecurity incident determined by the local
279 government to be of severity level 3, 4, or 5 as provided in s.
280 282.318(3)(c) to the Cybersecurity Operations Center, the
281 Cybercrime Office of the Department of Law Enforcement, and the
282 sheriff who has jurisdiction over the local government as soon
283 as possible but no later than 48 hours after discovery of the
284 cybersecurity incident and no later than 12 hours after
285 discovery of the ransomware incident. The report must contain
286 the information required in paragraph (a).

287 2. The Cybersecurity Operations Center shall notify the
288 President of the Senate and the Speaker of the House of
289 Representatives of any severity level 3, 4, or 5 incident as
290 soon as possible but no later than 12 hours after receiving a
291 local government's incident report. The notification must
292 include a high-level description of the incident and the likely
293 effects.

294 (c) A local government may report a cybersecurity incident
295 determined by the local government to be of severity level 1 or
296 2 as provided in s. 282.318(3)(c) to the Cybersecurity
297 Operations Center, the Cybercrime Office of the Department of
298 Law Enforcement, and the sheriff who has jurisdiction over the
299 local government. The report shall contain the information
300 required in paragraph (a).



272518

301 (d) The Cybersecurity Operations Center shall provide a
302 consolidated incident report on a quarterly basis to the
303 President of the Senate, the Speaker of the House of
304 Representatives, and the Florida Cybersecurity Advisory Council.
305 The report provided to the Florida Cybersecurity Advisory
306 Council may not contain the name of any local government,
307 network information, or system identifying information but must
308 contain sufficient relevant information to allow the Florida
309 Cybersecurity Advisory Council to fulfill its responsibilities
310 as required in s. 282.319(9).

311 (6) AFTER-ACTION REPORT.—A local government must submit to
312 the Florida Digital Service, within 1 week after the remediation
313 of a cybersecurity incident or ransomware incident, an after-
314 action report that summarizes the incident, the incident's
315 resolution, and any insights gained as a result of the incident.
316 By December 1, 2022, the Florida Digital Service shall establish
317 guidelines and processes for submitting an after-action report.

318 Section 4. Section 282.3186, Florida Statutes, is created
319 to read:

320 282.3186 Ransomware incident compliance.—A state agency as
321 defined in s. 282.318(2), a county, or a municipality
322 experiencing a ransomware incident may not pay or otherwise
323 comply with a ransom demand.

324 Section 5. Subsection (2) of section 282.319, Florida
325 Statutes, is amended, and paragraphs (g) and (h) are added to
326 subsection (9) and subsections (12) and (13) are added to that
327 section, to read:

328 282.319 Florida Cybersecurity Advisory Council.—

329 (2) The purpose of the council is to:



330 (a) Assist state agencies in protecting their information
331 technology resources from ~~cyber~~ cybersecurity threats and
332 incidents.

333 (b) Advise counties and municipalities on cybersecurity,
334 including cybersecurity threats, trends, and best practices.

335 (9) The council shall meet at least quarterly to:

336 (g) Review information relating to cybersecurity incidents
337 and ransomware incidents to determine commonalities and develop
338 best practice recommendations for state agencies, counties, and
339 municipalities.

340 (h) Recommend any additional information that a county or
341 municipality should report to the Florida Digital Service as
342 part of its cybersecurity incident or ransomware incident
343 notification pursuant to s. 282.3185.

344 (12) Beginning December 1, 2022, and each December 1
345 thereafter, the council shall submit to the Governor, the
346 President of the Senate, and the Speaker of the House of
347 Representatives a comprehensive report that includes data,
348 trends, analysis, findings, and recommendations for state and
349 local action regarding ransomware incidents. At a minimum, the
350 report must include:

351 (a) Descriptive statistics including the amount of ransom
352 requested, duration of the ransomware incident, and overall
353 monetary cost to taxpayers of the ransomware incident.

354 (b) A detailed statistical analysis of the circumstances
355 that led to the ransomware incident which does not include the
356 name of the state agency, county, or municipality; network
357 information; or system identifying information.

358 (c) A detailed statistical analysis of the level of



359 cybersecurity employee training and frequency of data backup for
360 the state agency, county, or municipality that reported the
361 ransomware incident.

362 (d) Specific issues identified with current policies,
363 procedures, rules, or statutes and recommendations to address
364 such issues.

365 (e) Any other recommendations to prevent ransomware
366 incidents.

367 (13) For purposes of this section, the term "state agency"
368 has the same meaning as provided in s. 282.318(2).

369 Section 6. Section 815.062, Florida Statutes, is created to
370 read:

371 815.062 Offenses against governmental entities.-

372 (1) As used in this section, the term "governmental entity"
373 means any official, officer, commission, board, authority,
374 council, committee, or department of the executive, judicial, or
375 legislative branch of state government; any state university; or
376 any county or municipality, special district, water management
377 district, or other political subdivision of the state.

378 (2) A person who willfully, knowingly, and without
379 authorization introduces a computer contaminant that gains
380 unauthorized access to, encrypts, modifies, or otherwise renders
381 unavailable data, programs, or supporting documentation residing
382 or existing within a computer, computer system, computer
383 network, or electronic device owned or operated by a
384 governmental entity and demands a ransom to prevent the
385 publication of or restore access to the data, programs, or
386 supporting documentation or to otherwise remediate the impact of
387 the computer contaminant commits a felony of the first degree,



272518

388 punishable as provided in s. 775.082, s. 775.083, or s. 775.084.

389 (3) An employee or contractor of a governmental entity with
390 access to the governmental entity's network who willfully and
391 knowingly aids or abets another in the commission of a violation
392 of subsection (2) commits a felony of the first degree,
393 punishable as provided in s. 775.082, s. 775.083, or s. 775.084.

394 (4) In addition to any other penalty imposed, a person
395 convicted of a violation of this section must pay a fine equal
396 to twice the amount of the ransom demand. Moneys recovered under
397 this subsection shall be deposited into the General Revenue
398 Fund.

399 Section 7. The Legislature finds and declares that this act
400 fulfills an important state interest.

401 Section 8. This act shall take effect July 1, 2022.

402

403 ===== T I T L E A M E N D M E N T =====

404 And the title is amended as follows:

405 Delete everything before the enacting clause
406 and insert:

407 A bill to be entitled
408 An act relating to cybersecurity; amending s.
409 282.0041, F.S.; revising a definition and defining the
410 term "ransomware incident"; amending s. 282.318, F.S.;
411 requiring the Department of Management Services,
412 acting through the Florida Digital Service, to develop
413 and publish guidelines and processes for reporting
414 cybersecurity incidents; requiring state agencies to
415 report ransomware incidents and certain cybersecurity
416 incidents to certain entities within specified



417 timeframes; requiring the Cybersecurity Operations
418 Center to provide certain notifications to the
419 Legislature within a specified timeframe; requiring
420 the Cybersecurity Operations Center to quarterly
421 provide certain reports to the Legislature and the
422 Florida Cybersecurity Advisory Council; requiring the
423 department, acting through the Florida Digital
424 Service, to develop and publish guidelines and
425 processes by a specified date for submitting after-
426 action reports and annually provide cybersecurity
427 training to certain persons; requiring state agency
428 heads to annually provide cybersecurity awareness
429 training to certain persons; requiring state agencies
430 to report cybersecurity incidents and ransomware
431 incidents in compliance with certain procedures and
432 timeframes; requiring state agency heads to submit
433 certain after-action reports to the Florida Digital
434 Service within a specified timeframe; creating s.
435 282.3185, F.S.; providing a short title; defining the
436 term "local government"; requiring the Florida Digital
437 Service to develop certain cybersecurity training
438 curricula; requiring certain persons to complete
439 certain cybersecurity training within a specified
440 timeframe and annually thereafter; authorizing the
441 Florida Digital Service to provide a certain training
442 in collaboration with certain entities; requiring
443 certain local governments to adopt certain
444 cybersecurity standards by specified dates; requiring
445 local governments to provide a certain notification to



272518

446 the Florida Digital Service and certain entities;
447 providing notification requirements; requiring local
448 governments to report ransomware incidents and certain
449 cybersecurity incidents to certain entities within
450 specified timeframes; requiring the Cybersecurity
451 Operations Center to provide a certain notification to
452 the Legislature within a specified timeframe;
453 authorizing local governments to report certain
454 cybersecurity incidents to certain entities; requiring
455 the Cybersecurity Operations Center to quarterly
456 provide certain reports to the Legislature and the
457 Florida Cybersecurity Advisory Council; requiring
458 local governments to submit after-action reports
459 containing certain information to the Florida Digital
460 Service within a specified timeframe; requiring the
461 Florida Digital Service to establish certain
462 guidelines and processes by a specified date; creating
463 s. 282.3186, F.S.; prohibiting certain entities from
464 paying or otherwise complying with a ransom demand;
465 amending s. 282.319, F.S.; revising the purpose of the
466 Florida Cybersecurity Advisory Council to include
467 advising counties and municipalities on cybersecurity;
468 requiring the council to meet at least quarterly to
469 review certain information and develop and make
470 certain recommendations; requiring the council to
471 annually submit to the Governor and the Legislature a
472 certain ransomware incident report beginning on a
473 specified date; providing requirements for the report;
474 defining the term "state agency"; creating s. 815.062,



272518

475 F.S.; defining the term "governmental entity";
476 prohibiting certain persons from introducing computer
477 contaminants in order to procure a ransom; prohibiting
478 certain employees or contractors from aiding or
479 abetting another to introduce computer contaminants in
480 order to procure a ransom; providing criminal
481 penalties; requiring a person convicted of certain
482 offenses to pay a certain fine; requiring deposit of
483 certain moneys in the General Revenue Fund; providing
484 a legislative finding and declaration of an important
485 state interest; providing an effective date.