

By the Committees on Appropriations; and Military and Veterans Affairs, Space, and Domestic Security; and Senator Hutson

576-03523-22

20221670c2

1 A bill to be entitled
2 An act relating to cybersecurity; amending s.
3 282.0041, F.S.; revising a definition and defining the
4 term "ransomware incident"; amending s. 282.318, F.S.;
5 requiring the Department of Management Services,
6 acting through the Florida Digital Service, to develop
7 and publish guidelines and processes for reporting
8 cybersecurity incidents; requiring state agencies to
9 report ransomware incidents and certain cybersecurity
10 incidents to certain entities within specified
11 timeframes; requiring the Cybersecurity Operations
12 Center to provide certain notifications to the
13 Legislature within a specified timeframe; requiring
14 the Cybersecurity Operations Center to quarterly
15 provide certain reports to the Legislature and the
16 Florida Cybersecurity Advisory Council; requiring the
17 department, acting through the Florida Digital
18 Service, to develop and publish guidelines and
19 processes by a specified date for submitting after-
20 action reports and annually provide cybersecurity
21 training to certain persons; requiring state agency
22 heads to annually provide cybersecurity awareness
23 training to certain persons; requiring state agencies
24 to report cybersecurity incidents and ransomware
25 incidents in compliance with certain procedures and
26 timeframes; requiring state agency heads to submit
27 certain after-action reports to the Florida Digital
28 Service within a specified timeframe; creating s.
29 282.3185, F.S.; providing a short title; defining the

576-03523-22

20221670c2

30 term "local government"; requiring the Florida Digital
31 Service to develop certain cybersecurity training
32 curricula; requiring certain persons to complete
33 certain cybersecurity training within a specified
34 timeframe and annually thereafter; authorizing the
35 Florida Digital Service to provide a certain training
36 in collaboration with certain entities; requiring
37 certain local governments to adopt certain
38 cybersecurity standards by specified dates; requiring
39 local governments to provide a certain notification to
40 the Florida Digital Service and certain entities;
41 providing notification requirements; requiring local
42 governments to report ransomware incidents and certain
43 cybersecurity incidents to certain entities within
44 specified timeframes; requiring the Cybersecurity
45 Operations Center to provide a certain notification to
46 the Legislature within a specified timeframe;
47 authorizing local governments to report certain
48 cybersecurity incidents to certain entities; requiring
49 the Cybersecurity Operations Center to quarterly
50 provide certain reports to the Legislature and the
51 Florida Cybersecurity Advisory Council; requiring
52 local governments to submit after-action reports
53 containing certain information to the Florida Digital
54 Service within a specified timeframe; requiring the
55 Florida Digital Service to establish certain
56 guidelines and processes by a specified date; creating
57 s. 282.3186, F.S.; prohibiting certain entities from
58 paying or otherwise complying with a ransom demand;

576-03523-22

20221670c2

59 amending s. 282.319, F.S.; revising the purpose of the
60 Florida Cybersecurity Advisory Council to include
61 advising counties and municipalities on cybersecurity;
62 requiring the council to meet at least quarterly to
63 review certain information and develop and make
64 certain recommendations; requiring the council to
65 annually submit to the Governor and the Legislature a
66 certain ransomware incident report beginning on a
67 specified date; providing requirements for the report;
68 defining the term "state agency"; creating s. 815.062,
69 F.S.; defining the term "governmental entity";
70 prohibiting certain persons from introducing computer
71 contaminants in order to procure a ransom; prohibiting
72 certain employees or contractors from aiding or
73 abetting another to introduce computer contaminants in
74 order to procure a ransom; providing criminal
75 penalties; requiring a person convicted of certain
76 offenses to pay a certain fine; requiring deposit of
77 certain moneys in the General Revenue Fund; providing
78 a legislative finding and declaration of an important
79 state interest; providing an effective date.

80

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

82

83 Section 1. Present subsections (28) through (37) of section
84 282.0041, Florida Statutes, are redesignated as subsections (29)
85 through (38), respectively, a new subsection (28) is added to
86 that section, and subsection (19) of that section is amended, to
87 read:

576-03523-22

20221670c2

88 282.0041 Definitions.—As used in this chapter, the term:

89 (19) "Incident" means a violation or imminent threat of
90 violation, whether such violation is accidental or deliberate,
91 of information technology resources, security, policies, or
92 practices. An imminent threat of violation refers to a situation
93 in which a the state agency, county, or municipality has a
94 factual basis for believing that a specific incident is about to
95 occur.

96 (28) "Ransomware incident" means a malicious cybersecurity
97 incident in which a person or entity introduces software that
98 gains unauthorized access to or encrypts, modifies, or otherwise
99 renders unavailable a state agency's, county's, or
100 municipality's data and thereafter the person or entity demands
101 a ransom to prevent the publication of the data, restore access
102 to the data, or otherwise remediate the impact of the software.

103 Section 2. Paragraphs (c) and (g) of subsection (3) and
104 paragraphs (i) and (j) of subsection (4) of section 282.318,
105 Florida Statutes, are amended, and paragraph (k) is added to
106 subsection (4) of that section, to read:

107 282.318 Cybersecurity.—

108 (3) The department, acting through the Florida Digital
109 Service, is the lead entity responsible for establishing
110 standards and processes for assessing state agency cybersecurity
111 risks and determining appropriate security measures. Such
112 standards and processes must be consistent with generally
113 accepted technology best practices, including the National
114 Institute for Standards and Technology Cybersecurity Framework,
115 for cybersecurity. The department, acting through the Florida
116 Digital Service, shall adopt rules that mitigate risks;

576-03523-22

20221670c2

117 safeguard state agency digital assets, data, information, and
118 information technology resources to ensure availability,
119 confidentiality, and integrity; and support a security
120 governance framework. The department, acting through the Florida
121 Digital Service, shall also:

122 (c) Develop and publish for use by state agencies a
123 cybersecurity governance framework that, at a minimum, includes
124 guidelines and processes for:

125 1. Establishing asset management procedures to ensure that
126 an agency's information technology resources are identified and
127 managed consistent with their relative importance to the
128 agency's business objectives.

129 2. Using a standard risk assessment methodology that
130 includes the identification of an agency's priorities,
131 constraints, risk tolerances, and assumptions necessary to
132 support operational risk decisions.

133 3. Completing comprehensive risk assessments and
134 cybersecurity audits, which may be completed by a private sector
135 vendor, and submitting completed assessments and audits to the
136 department.

137 4. Identifying protection procedures to manage the
138 protection of an agency's information, data, and information
139 technology resources.

140 5. Establishing procedures for accessing information and
141 data to ensure the confidentiality, integrity, and availability
142 of such information and data.

143 6. Detecting threats through proactive monitoring of
144 events, continuous security monitoring, and defined detection
145 processes.

576-03523-22

20221670c2

146 7. Establishing agency cybersecurity incident response
147 teams and describing their responsibilities for responding to
148 cybersecurity incidents, including breaches of personal
149 information containing confidential or exempt data.

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

153 9. Establishing a cybersecurity incident reporting process
154 that includes procedures ~~and tiered reporting timeframes~~ for
155 notifying the department and the Department of Law Enforcement
156 of cybersecurity incidents. ~~The tiered reporting timeframes~~
157 ~~shall be based upon the level of severity of the cybersecurity~~
158 ~~incidents being reported.~~

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

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

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

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

576-03523-22

20221670c2

175 (IV) Level 2 is a medium-level incident that may impact
176 public health or safety; national, state, or local security;
177 economic security; civil liberties; or public confidence.

178 (V) Level 1 is a low-level incident that is unlikely to
179 impact public health or safety; national, state, or local
180 security; economic security; civil liberties; or public
181 confidence.

182 b. The cybersecurity incident reporting process must
183 specify the information that must be reported by a state agency
184 following a cybersecurity incident or ransomware incident,
185 which, at a minimum, must include the following:

186 (I) A summary of the facts surrounding the cybersecurity
187 incident or ransomware incident.

188 (II) The date on which the state agency most recently
189 backed up its data, the physical location of the backup, if the
190 backup was affected, and if the backup was created using cloud
191 computing.

192 (III) The types of data compromised by the cybersecurity
193 incident or ransomware incident.

194 (IV) The estimated fiscal impact of the cybersecurity
195 incident or ransomware incident.

196 (V) In the case of a ransomware incident, the details of
197 the ransom demanded.

198 c.(I) A state agency shall report all ransomware incidents
199 and any cybersecurity incident determined by the state agency to
200 be of severity level 3, 4, or 5 to the Cybersecurity Operations
201 Center and the Cybercrime Office of the Department of Law
202 Enforcement as soon as possible but no later than 48 hours after
203 discovery of the cybersecurity incident and no later than 12

576-03523-22

20221670c2

204 hours after discovery of the ransomware incident. The report
205 must contain the information required in sub-subparagraph b.

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

212 d. A state agency shall report a cybersecurity incident
213 determined by the state agency to be of severity level 1 or 2 to
214 the Cybersecurity Operations Center and the Cybercrime Office of
215 the Department of Law Enforcement as soon as possible. The
216 report must contain the information required in sub-subparagraph
217 b.

218 e. The Cybersecurity Operations Center shall provide a
219 consolidated incident report on a quarterly basis to the
220 President of the Senate, the Speaker of the House of
221 Representatives, and the Florida Cybersecurity Advisory Council.
222 The report provided to the Florida Cybersecurity Advisory
223 Council may not contain the name of any agency, network
224 information, or system identifying information but must contain
225 sufficient relevant information to allow the Florida
226 Cybersecurity Advisory Council to fulfill its responsibilities
227 as required in s. 282.319(9).

228 10. Incorporating information obtained through detection
229 and response activities into the agency's cybersecurity incident
230 response plans.

231 11. Developing agency strategic and operational
232 cybersecurity plans required pursuant to this section.

576-03523-22

20221670c2

233 12. Establishing the managerial, operational, and technical
234 safeguards for protecting state government data and information
235 technology resources that align with the state agency risk
236 management strategy and that protect the confidentiality,
237 integrity, and availability of information and data.

238 13. Establishing procedures for procuring information
239 technology commodities and services that require the commodity
240 or service to meet the National Institute of Standards and
241 Technology Cybersecurity Framework.

242 14. Submitting after-action reports following a
243 cybersecurity incident or ransomware incident. Such guidelines
244 and processes for submitting after-action reports must be
245 developed and published by December 1, 2022.

246 (g) Annually provide cybersecurity training to all state
247 agency technology professionals and employees with access to
248 highly sensitive information which ~~that~~ develops, assesses, and
249 documents competencies by role and skill level. The
250 cybersecurity training curriculum must include training on the
251 identification of each cybersecurity incident severity level
252 referenced in sub-subparagraph (c)9.a. The training may be
253 provided in collaboration with the Cybercrime Office of the
254 Department of Law Enforcement, a private sector entity, or an
255 institution of the State University System.

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

257 (i) Provide cybersecurity awareness training to all state
258 agency employees within ~~in the first~~ 30 days after commencing
259 employment, and annually thereafter, concerning cybersecurity
260 risks and the responsibility of employees to comply with
261 policies, standards, guidelines, and operating procedures

576-03523-22

20221670c2

262 adopted by the state agency to reduce those risks. The training
263 may be provided in collaboration with the Cybercrime Office of
264 the Department of Law Enforcement, a private sector entity, or
265 an institution of the State University System.

266 (j) Develop a process for detecting, reporting, and
267 responding to threats, breaches, or cybersecurity incidents
268 which is consistent with the security rules, guidelines, and
269 processes established by the department through the Florida
270 Digital Service.

271 1. All cybersecurity incidents and ransomware incidents
272 ~~breaches~~ must be reported by state agencies. Such reports ~~to the~~
273 ~~Florida Digital Service within the department and the Cybercrime~~
274 ~~Office of the Department of Law Enforcement and~~ must comply with
275 the notification procedures and reporting timeframes established
276 pursuant to paragraph (3) (c).

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

279 (k) Submit to the Florida Digital Service, within 1 week
280 after the remediation of a cybersecurity incident or ransomware
281 incident, an after-action report that summarizes the incident,
282 the incident's resolution, and any insights gained as a result
283 of the incident.

284 Section 3. Section 282.3185, Florida Statutes, is created
285 to read:

286 282.3185 Local government cybersecurity.—

287 (1) SHORT TITLE.—This section may be cited as the "Local
288 Government Cybersecurity Act."

289 (2) DEFINITION.—As used in this section, the term "local
290 government" means any county or municipality.

576-03523-22

20221670c2

291 (3) CYBERSECURITY TRAINING.—

292 (a) The Florida Digital Service shall:

293 1. Develop a basic cybersecurity training curriculum for
294 local government employees. All local government employees with
295 access to the local government's network must complete the basic
296 cybersecurity training within 30 days after commencing
297 employment and annually thereafter.

298 2. Develop an advanced cybersecurity training curriculum
299 for local governments which is consistent with the cybersecurity
300 training required under s. 282.318(3)(g). All local government
301 technology professionals and employees with access to highly
302 sensitive information must complete the advanced cybersecurity
303 training within 30 days after commencing employment and annually
304 thereafter.

305 (b) The Florida Digital Service may provide the
306 cybersecurity training required by this subsection in
307 collaboration with the Cybercrime Office of the Department of
308 Law Enforcement, a private sector entity, or an institution of
309 the State University System.

310 (4) CYBERSECURITY STANDARDS.—

311 (a) Each local government shall adopt cybersecurity
312 standards that safeguard its data, information technology, and
313 information technology resources to ensure availability,
314 confidentiality, and integrity. The cybersecurity standards must
315 be consistent with generally accepted best practices for
316 cybersecurity, including the National Institute of Standards and
317 Technology Cybersecurity Framework.

318 (b) Each county with a population of 75,000 or more must
319 adopt the cybersecurity standards required by this subsection by

576-03523-22

20221670c2

320 January 1, 2024. Each county with a population of less than
321 75,000 must adopt the cybersecurity standards required by this
322 subsection by January 1, 2025.

323 (c) Each municipality with a population of 25,000 or more
324 must adopt the cybersecurity standards required by this
325 subsection by January 1, 2024. Each municipality with a
326 population of less than 25,000 must adopt the cybersecurity
327 standards required by this subsection by January 1, 2025.

328 (d) Each local government shall notify the Florida Digital
329 Service of its compliance with this subsection as soon as
330 possible.

331 (5) INCIDENT NOTIFICATION.—

332 (a) A local government shall provide notification of a
333 cybersecurity incident or ransomware incident to the
334 Cybersecurity Operations Center, Cybercrime Office of the
335 Department of Law Enforcement, and sheriff who has jurisdiction
336 over the local government in accordance with paragraph (b). The
337 notification must include, at a minimum, the following
338 information:

339 1. A summary of the facts surrounding the cybersecurity
340 incident or ransomware incident.

341 2. The date on which the local government most recently
342 backed up its data, the physical location of the backup, if the
343 backup was affected, and if the backup was created using cloud
344 computing.

345 3. The types of data compromised by the cybersecurity
346 incident or ransomware incident.

347 4. The estimated fiscal impact of the cybersecurity
348 incident or ransomware incident.

576-03523-22

20221670c2

349 5. In the case of a ransomware incident, the details of the
350 ransom demanded.

351 6. A statement requesting or declining assistance from the
352 Cybersecurity Operations Center, the Cybercrime Office of the
353 Department of Law Enforcement, or the sheriff who has
354 jurisdiction over the local government.

355 (b)1. A local government shall report all ransomware
356 incidents and any cybersecurity incident determined by the local
357 government to be of severity level 3, 4, or 5 as provided in s.
358 282.318(3)(c) to the Cybersecurity Operations Center, the
359 Cybercrime Office of the Department of Law Enforcement, and the
360 sheriff who has jurisdiction over the local government as soon
361 as possible but no later than 48 hours after discovery of the
362 cybersecurity incident and no later than 12 hours after
363 discovery of the ransomware incident. The report must contain
364 the information required in paragraph (a).

365 2. The Cybersecurity Operations Center shall notify the
366 President of the Senate and the Speaker of the House of
367 Representatives of any severity level 3, 4, or 5 incident as
368 soon as possible but no later than 12 hours after receiving a
369 local government's incident report. The notification must
370 include a high-level description of the incident and the likely
371 effects.

372 (c) A local government may report a cybersecurity incident
373 determined by the local government to be of severity level 1 or
374 2 as provided in s. 282.318(3)(c) to the Cybersecurity
375 Operations Center, the Cybercrime Office of the Department of
376 Law Enforcement, and the sheriff who has jurisdiction over the
377 local government. The report shall contain the information

576-03523-22

20221670c2

378 required in paragraph (a).

379 (d) The Cybersecurity Operations Center shall provide a
380 consolidated incident report on a quarterly basis to the
381 President of the Senate, the Speaker of the House of
382 Representatives, and the Florida Cybersecurity Advisory Council.
383 The report provided to the Florida Cybersecurity Advisory
384 Council may not contain the name of any local government,
385 network information, or system identifying information but must
386 contain sufficient relevant information to allow the Florida
387 Cybersecurity Advisory Council to fulfill its responsibilities
388 as required in s. 282.319(9).

389 (6) AFTER-ACTION REPORT.—A local government must submit to
390 the Florida Digital Service, within 1 week after the remediation
391 of a cybersecurity incident or ransomware incident, an after-
392 action report that summarizes the incident, the incident's
393 resolution, and any insights gained as a result of the incident.
394 By December 1, 2022, the Florida Digital Service shall establish
395 guidelines and processes for submitting an after-action report.

396 Section 4. Section 282.3186, Florida Statutes, is created
397 to read:

398 282.3186 Ransomware incident compliance.—A state agency as
399 defined in s. 282.318(2), a county, or a municipality
400 experiencing a ransomware incident may not pay or otherwise
401 comply with a ransom demand.

402 Section 5. Subsection (2) of section 282.319, Florida
403 Statutes, is amended, paragraphs (g) and (h) are added to
404 subsection (9) of that section, and subsections (12) and (13)
405 are added to that section, to read:

406 282.319 Florida Cybersecurity Advisory Council.—

576-03523-22

20221670c2

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

408 (a) Assist state agencies in protecting their information
409 technology resources from cybersecurity ~~cyber~~ threats and
410 incidents.

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

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

414 (g) Review information relating to cybersecurity incidents
415 and ransomware incidents to determine commonalities and develop
416 best practice recommendations for state agencies, counties, and
417 municipalities.

418 (h) Recommend any additional information that a county or
419 municipality should report to the Florida Digital Service as
420 part of its cybersecurity incident or ransomware incident
421 notification pursuant to s. 282.3185.

422 (12) Beginning December 1, 2022, and each December 1
423 thereafter, the council shall submit to the Governor, the
424 President of the Senate, and the Speaker of the House of
425 Representatives a comprehensive report that includes data,
426 trends, analysis, findings, and recommendations for state and
427 local action regarding ransomware incidents. At a minimum, the
428 report must include:

429 (a) Descriptive statistics including the amount of ransom
430 requested, duration of the ransomware incident, and overall
431 monetary cost to taxpayers of the ransomware incident.

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

576-03523-22

20221670c2

436 (c) A detailed statistical analysis of the level of
437 cybersecurity employee training and frequency of data backup for
438 the state agency, county, or municipality that reported the
439 ransomware incident.

440 (d) Specific issues identified with current policies,
441 procedures, rules, or statutes and recommendations to address
442 such issues.

443 (e) Any other recommendations to prevent ransomware
444 incidents.

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

447 Section 6. Section 815.062, Florida Statutes, is created to
448 read:

449 815.062 Offenses against governmental entities.-

450 (1) As used in this section, the term "governmental entity"
451 means any official, officer, commission, board, authority,
452 council, committee, or department of the executive, judicial, or
453 legislative branch of state government; any state university; or
454 any county or municipality, special district, water management
455 district, or other political subdivision of the state.

456 (2) A person who willfully, knowingly, and without
457 authorization introduces a computer contaminant that gains
458 unauthorized access to, encrypts, modifies, or otherwise renders
459 unavailable data, programs, or supporting documentation residing
460 or existing within a computer, computer system, computer
461 network, or electronic device owned or operated by a
462 governmental entity and demands a ransom to prevent the
463 publication of or restore access to the data, programs, or
464 supporting documentation or to otherwise remediate the impact of

576-03523-22

20221670c2

465 the computer contaminant commits a felony of the first degree,
466 punishable as provided in s. 775.082, s. 775.083, or s. 775.084.

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

472 (4) In addition to any other penalty imposed, a person
473 convicted of a violation of this section must pay a fine equal
474 to twice the amount of the ransom demand. Moneys recovered under
475 this subsection shall be deposited into the General Revenue
476 Fund.

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

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