

FOR CONSIDERATION By the Committee on Appropriations

576-02763A-23

20232508pb

1 A bill to be entitled
2 An act relating to state cybersecurity operations;
3 providing for a type two transfer of the Cybersecurity
4 Operations Center and related services, including the
5 position of the state chief information security
6 officer, from the Florida Digital Service within the
7 Department of Management Services to the Department of
8 Law Enforcement; amending s. 282.318, F.S.; requiring
9 the Department of Management Services, acting through
10 the Florida Digital Service, to perform specified
11 actions relating to state agency cybersecurity risks;
12 requiring the Department of Management Services to
13 perform specified actions in consultation with and
14 with approval from the state chief information
15 security officer; requiring that the cybersecurity
16 governance framework minimum guidelines be consistent
17 with the state cybersecurity strategic plan;
18 specifying that the Department of Law Enforcement is
19 the lead entity responsible for enterprise
20 cybersecurity operations; requiring the Department of
21 Law Enforcement to designate a state chief information
22 security officer; providing the qualifications for and
23 the responsibilities of the state chief information
24 security officer; requiring that the state chief
25 information security officer be notified of all
26 confirmed or suspected incidents involving, or threats
27 to, state agency information; requiring the state
28 chief information security officer to report such
29 incidents to the Governor and the state chief

576-02763A-23

20232508pb

30 information officer; requiring the Department of Law
31 Enforcement to develop, and annually update by a
32 specified date, a certain state cybersecurity
33 strategic plan; requiring the Department of Law
34 Enforcement to operate and maintain the Cybersecurity
35 Operations Center as part of the Florida Fusion
36 Center; requiring that the center be staffed with
37 specified personnel; requiring the center to
38 coordinate with the Florida Digital Service to support
39 state agencies and their responses to cybersecurity
40 incidents; requiring the Department of Law Enforcement
41 to review and approve, before publication, the
42 cybersecurity governance framework established by the
43 Florida Digital Service; requiring the Department of
44 Law Enforcement to review and approve all
45 cybersecurity training provided by or facilitated
46 through the Florida Digital Service; requiring the
47 Department of Law Enforcement to develop and publish
48 specified guidelines and processes for establishing a
49 cybersecurity incident reporting process for use by
50 state agencies; requiring the Florida Digital Service
51 to provide certain reports on a periodic basis to the
52 Legislature, the state chief information security
53 officer, and the Cybersecurity Advisory Council;
54 prohibiting the report transmitted to the advisory
55 council from containing certain information; requiring
56 state agency heads, in consultation with the
57 Cybersecurity Operations Center, the Cybercrime
58 Office, and the Florida Digital Service, to establish

576-02763A-23

20232508pb

59 an agency cybersecurity response team to respond to
60 cybersecurity incidents; requiring state agencies to
61 submit a corrective action plan to the Florida Digital
62 Service within a specified timeframe for all findings
63 confirmed by the state chief information security
64 officer; requiring that certain implementation plans
65 be submitted to the state chief information officer on
66 a periodic basis; requiring that a specified
67 comprehensive risk assessment be conducted annually;
68 providing that certain public records exemptions do
69 not apply to information made available to the
70 Cybersecurity Operations Center; providing that
71 certain mandatory cybersecurity awareness training
72 offered to state employees may be provided in
73 collaboration with the Cyber Security Operations
74 Center or the Florida Digital Service; conforming a
75 provision to changes made by the act; requiring state
76 agency heads to submit after-action reports to the
77 Department of Law Enforcement and other specified
78 entities; requiring that certain confidential and
79 exempt records be made available to the state chief
80 information officer; requiring the Department of Law
81 Enforcement to adopt specified rules; amending s.
82 282.3185, F.S.; requiring that certain cybersecurity
83 training programs developed by the Florida Digital
84 Service be approved by the state chief information
85 security officer; authorizing the Florida Digital
86 service to collaborate with the Cybersecurity
87 Operations Center to provide certain cybersecurity

576-02763A-23

20232508pb

88 training; requiring local governments to provide
89 notification of a cybersecurity or ransomware incident
90 to the Florida Digital Service and other entities
91 within a specified timeframe after the incident;
92 requiring local governments to provide a certain
93 report of cybersecurity incidents or ransomware
94 incidents of a specified severity level to the Florida
95 Digital Service and other entities; authorizing local
96 governments to provide a certain report of
97 cybersecurity incidents or ransomware incidents of a
98 specified severity level to the Florida Digital
99 Service; requiring the Florida Digital Service to
100 provide certain consolidated incident reports to the
101 state chief information security officer and other
102 entities; requiring the Florida Digital Service to
103 collaborate with the state chief information security
104 officer to establish guidelines and processes for
105 submitting after-action reports, by a specified date;
106 conforming a cross-reference; providing an effective
107 date.

108
109 Be It Enacted by the Legislature of the State of Florida:

110
111 Section 1. All positions, duties, functions, records,
112 existing contracts, administrative authority, administrative
113 rules, and unexpended balances of appropriations, allocations,
114 and other public funds relating to the Cybersecurity Operations
115 Center and related services, including the position of the state
116 chief information security officer, of the Florida Digital

576-02763A-23

20232508pb

117 Service within the Department of Management Services are
118 transferred by a type two transfer as defined in s. 20.06(2),
119 Florida Statutes, to the Department of Law Enforcement.

120 Section 2. Section 282.318, Florida Statutes, is amended to
121 read:

122 282.318 Cybersecurity.—

123 (1) This section may be cited as the "State Cybersecurity
124 Act."

125 (2) As used in this section, the term "state agency" has
126 the same meaning as provided in s. 282.0041, except that the
127 term includes the Department of Legal Affairs, the Department of
128 Agriculture and Consumer Services, and the Department of
129 Financial Services.

130 (3) The department, acting through the Florida Digital
131 Service, is the lead entity responsible for establishing
132 standards and processes for assessing state agency cybersecurity
133 risks ~~and determining appropriate security measures~~. Such
134 standards and processes must be consistent with generally
135 accepted technology best practices for cybersecurity, including
136 the National Institute for Standards and Technology
137 Cybersecurity Framework, ~~for cybersecurity~~. The department,
138 acting through the Florida Digital Service, shall:

139 (a) Assist state agencies in complying with this section.

140 (b) Annually review the strategic and operational
141 cybersecurity plans of state agencies for compliance with the
142 cybersecurity governance framework. The review of the plans must
143 include the following:

144 1. Providing findings to the state chief information
145 security officer for review and confirmation;

576-02763A-23

20232508pb

146 2. Notifying agencies of confirmed findings and the date by
147 which the agency must submit a corrective action plan;

148 3. Reviewing corrective action plans submitted by agencies;

149 4. Tracking and monitoring progress of the implementation
150 of corrective action plans; and

151 5. Annually submitting a report to the state chief
152 information security officer which includes, by agency,
153 completed reviews, any confirmed findings, a brief description
154 of corresponding corrective action plans, and the status of
155 corrective action plan implementation.

156 (c) Review state agency annual risk assessment findings and
157 corresponding remediation plans, including:

158 1. Tracking and monitoring the progress of the risk
159 assessment remediation plans; and

160 2. Annually submitting a report to the state chief
161 information security officer which includes, by agency, risk
162 assessment findings, a brief description of corresponding
163 remediation plans, and the status of remediation plan
164 implementation.

165 (d) Annually provide cybersecurity training for state
166 agency information security managers and computer security
167 incident response team members which includes training on
168 cybersecurity threats, trends, and best practices. The training
169 curriculum must be approved by the state chief information
170 security officer.

171 (e) Annually provide cybersecurity training to all state
172 agency technology professionals and employees with access to
173 highly sensitive information which develops, assesses, and
174 documents competencies by role and skill level. The

576-02763A-23

20232508pb

175 cybersecurity training curriculum must include training on the
176 identification of each cybersecurity incident severity level
177 referenced in subparagraph (5)(g)1. The training must be
178 approved by the state chief information security officer and may
179 be provided in collaboration with a private sector entity or an
180 institution of the State University System.

181 (4) The department, acting through the Florida Digital
182 Service, and in consultation with and with approval from the
183 state chief information security officer, shall:

184 (a) Adopt rules that mitigate risks; safeguard state agency
185 digital assets, data, information, and information technology
186 resources to ensure availability, confidentiality, and
187 integrity; and support a security governance framework. The
188 department, acting through the Florida Digital Service, shall
189 also:

190 ~~(a) Designate an employee of the Florida Digital Service as~~
191 ~~the state chief information security officer. The state chief~~
192 ~~information security officer must have experience and expertise~~
193 ~~in security and risk management for communications and~~
194 ~~information technology resources. The state chief information~~
195 ~~security officer is responsible for the development, operation,~~
196 ~~and oversight of cybersecurity for state technology systems. The~~
197 ~~state chief information security officer shall be notified of~~
198 ~~all confirmed or suspected incidents or threats of state agency~~
199 ~~information technology resources and must report such incidents~~
200 ~~or threats to the state chief information officer and the~~
201 ~~Governor.~~

202 ~~(b) Develop, and annually update by February 1, a statewide~~
203 ~~cybersecurity strategic plan that includes security goals and~~

576-02763A-23

20232508pb

204 ~~objectives for cybersecurity, including the identification and~~
205 ~~mitigation of risk, proactive protections against threats,~~
206 ~~tactical risk detection, threat reporting, and response and~~
207 ~~recovery protocols for a cyber incident.~~

208 (b) ~~(e)~~ Develop and publish for use by state agencies a
209 cybersecurity governance framework consistent with the state
210 cybersecurity strategic plan which ~~that~~, at a minimum, includes
211 guidelines and processes for:

212 1. Establishing asset management procedures to ensure that
213 an agency's information technology resources are identified and
214 managed consistent with their relative importance to the
215 agency's business objectives.

216 2. Using a standard risk assessment methodology that
217 includes the identification of an agency's priorities,
218 constraints, risk tolerances, and assumptions necessary to
219 support operational risk decisions.

220 ~~3. Completing comprehensive risk assessments and~~
221 ~~cybersecurity audits, which may be completed by a private sector~~
222 ~~vendor, and submitting completed assessments and audits to the~~
223 ~~department.~~

224 ~~3.4.~~ Identifying protection procedures to manage the
225 protection of an agency's information, data, and information
226 technology resources.

227 ~~4.5.~~ Establishing procedures for accessing information and
228 data to ensure the confidentiality, integrity, and availability
229 of such information and data.

230 ~~5.6.~~ Detecting threats through proactive monitoring of
231 events, continuous security monitoring, and defined detection
232 processes.

576-02763A-23

20232508pb

233 6.7. Establishing agency cybersecurity incident response
234 teams and describing their responsibilities for responding to
235 cybersecurity incidents, including breaches of personal
236 information containing confidential or exempt data.

237 7.8. Recovering information and data in response to a
238 cybersecurity incident. The recovery may include recommended
239 improvements to the agency processes, policies, or guidelines.

240 ~~9. Establishing a cybersecurity incident reporting process~~
241 ~~that includes procedures for notifying the department and the~~
242 ~~Department of Law Enforcement of cybersecurity incidents.~~

243 ~~a. The level of severity of the cybersecurity incident is~~
244 ~~defined by the National Cyber Incident Response Plan of the~~
245 ~~United States Department of Homeland Security as follows:~~

246 ~~(I) Level 5 is an emergency-level incident within the~~
247 ~~specified jurisdiction that poses an imminent threat to the~~
248 ~~provision of wide-scale critical infrastructure services;~~
249 ~~national, state, or local government security; or the lives of~~
250 ~~the country's, state's, or local government's residents.~~

251 ~~(II) Level 4 is a severe-level incident that is likely to~~
252 ~~result in a significant impact in the affected jurisdiction to~~
253 ~~public health or safety; national, state, or local security;~~
254 ~~economic security; or civil liberties.~~

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

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

576-02763A-23

20232508pb

262 ~~(V) Level 1 is a low-level incident that is unlikely to~~
263 ~~impact public health or safety; national, state, or local~~
264 ~~security; economic security; civil liberties; or public~~
265 ~~confidence.~~

266 ~~b. The cybersecurity incident reporting process must~~
267 ~~specify the information that must be reported by a state agency~~
268 ~~following a cybersecurity incident or ransomware incident,~~
269 ~~which, at a minimum, must include the following:~~

270 ~~(I) A summary of the facts surrounding the cybersecurity~~
271 ~~incident or ransomware incident.~~

272 ~~(II) The date on which the state agency most recently~~
273 ~~backed up its data; the physical location of the backup, if the~~
274 ~~backup was affected; and if the backup was created using cloud~~
275 ~~computing.~~

276 ~~(III) The types of data compromised by the cybersecurity~~
277 ~~incident or ransomware incident.~~

278 ~~(IV) The estimated fiscal impact of the cybersecurity~~
279 ~~incident or ransomware incident.~~

280 ~~(V) In the case of a ransomware incident, the details of~~
281 ~~the ransom demanded.~~

282 ~~e.(I) A state agency shall report all ransomware incidents~~
283 ~~and any cybersecurity incident determined by the state agency to~~
284 ~~be of severity level 3, 4, or 5 to the Cybersecurity Operations~~
285 ~~Center and the Cybercrime Office of the Department of Law~~
286 ~~Enforcement as soon as possible but no later than 48 hours after~~
287 ~~discovery of the cybersecurity incident and no later than 12~~
288 ~~hours after discovery of the ransomware incident. The report~~
289 ~~must contain the information required in sub-subparagraph b.~~

290 ~~(II) The Cybersecurity Operations Center shall notify the~~

576-02763A-23

20232508pb

291 ~~President of the Senate and the Speaker of the House of~~
292 ~~Representatives of any severity level 3, 4, or 5 incident as~~
293 ~~soon as possible but no later than 12 hours after receiving a~~
294 ~~state agency's incident report. The notification must include a~~
295 ~~high-level description of the incident and the likely effects.~~

296 ~~d. A state agency shall report a cybersecurity incident~~
297 ~~determined by the state agency to be of severity level 1 or 2 to~~
298 ~~the Cybersecurity Operations Center and the Cybercrime Office of~~
299 ~~the Department of Law Enforcement as soon as possible. The~~
300 ~~report must contain the information required in sub-subparagraph~~
301 ~~b.~~

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

312 ~~8.10.~~ Incorporating information obtained through detection
313 and response activities into the agency's cybersecurity incident
314 response plans.

315 ~~9.11.~~ Developing agency strategic and operational
316 cybersecurity plans required pursuant to this section.

317 ~~10.12.~~ Establishing the managerial, operational, and
318 technical safeguards for protecting state government data and
319 information technology resources that align with the state

576-02763A-23

20232508pb

320 agency risk management strategy and that protect the
321 confidentiality, integrity, and availability of information and
322 data.

323 ~~11.13.~~ Establishing procedures for procuring information
324 technology commodities and services that require the commodity
325 or service to meet the National Institute of Standards and
326 Technology Cybersecurity Framework.

327 ~~12.14.~~ Submitting after-action reports following a
328 cybersecurity incident or ransomware incident. Such guidelines
329 and processes for submitting after-action reports must be
330 developed and published by December 1, 2023 ~~2022~~.

331 ~~(d) Assist state agencies in complying with this section.~~

332 ~~(e) In collaboration with the Cybercrime Office of the~~
333 ~~Department of Law Enforcement, annually provide training for~~
334 ~~state agency information security managers and computer security~~
335 ~~incident response team members that contains training on~~
336 ~~cybersecurity, including cybersecurity threats, trends, and best~~
337 ~~practices.~~

338 ~~(f) Annually review the strategic and operational~~
339 ~~cybersecurity plans of state agencies.~~

340 ~~(g) Annually provide cybersecurity training to all state~~
341 ~~agency technology professionals and employees with access to~~
342 ~~highly sensitive information which develops, assesses, and~~
343 ~~documents competencies by role and skill level. The~~
344 ~~cybersecurity training curriculum must include training on the~~
345 ~~identification of each cybersecurity incident severity level~~
346 ~~referenced in sub-subparagraph (c)9.a. The training may be~~
347 ~~provided in collaboration with the Cybercrime Office of the~~
348 ~~Department of Law Enforcement, a private sector entity, or an~~

576-02763A-23

20232508pb

349 ~~institution of the State University System.~~

350 (5) The Department of Law Enforcement is the lead entity
351 responsible for enterprise cybersecurity operations and as the
352 lead entity, the Department of Law Enforcement shall:

353 (a) Designate an employee as the state chief information
354 security officer. The state chief information security officer
355 must have experience and expertise in security and risk
356 management for communications and information technology
357 resources. The state chief information security officer is
358 responsible for the development, operation, and oversight of
359 cybersecurity for state technology systems. The state chief
360 information security officer must be notified of all confirmed
361 or suspected incidents involving, or threats to, state agency
362 information technology resources and must report such incidents
363 or threats to the Governor and the state chief information
364 officer.

365 (b) Develop, and annually update by February 1, a state
366 cybersecurity strategic plan that includes security goals and
367 objectives for cybersecurity, including the identification and
368 mitigation of risk, proactive protections against threats,
369 tactical risk detection, threat reporting, and response and
370 recovery protocols for a cyber incident.

371 (c) ~~(h)~~ Operate and maintain a Cybersecurity Operations
372 Center as part of the Florida Fusion Center led by the state
373 chief information security officer, which must be primarily
374 virtual and ~~staffed with tactical detection and incident~~
375 response personnel. The Cybersecurity Operations Center shall
376 serve as a clearinghouse for threat information and coordinate
377 with the Florida Digital Service Department of Law Enforcement

576-02763A-23

20232508pb

378 to support state agencies and their response to any confirmed or
379 suspected cybersecurity incident.

380 (d) Before publication, review and approve the
381 cybersecurity governance framework established by the Florida
382 Digital Service.

383 (e) Review and approve all cybersecurity training provided
384 by or facilitated through the Florida Digital Service within the
385 Department of Management Services.

386 (f)~~(i)~~ Lead an Emergency Support Function, ESF CYBER, under
387 the state comprehensive emergency management plan as described
388 in s. 252.35.

389 (g) Develop and publish for use by state agencies
390 guidelines and processes for establishing a cybersecurity
391 incident reporting process that includes procedures and secure
392 communication mechanisms for notifying the Department of Law
393 Enforcement, the Florida Digital Service, and other stakeholders
394 of cybersecurity incidents.

395 1. The level of severity of the cybersecurity incidents is
396 defined by the National Cyber Incident Response Plan of the
397 United States Department of Homeland Security as follows:

398 a. Level 5 is an emergency-level incident within the
399 specified jurisdiction which poses an imminent threat to the
400 provision of wide-scale critical infrastructure services;
401 national, state, or local government security; or the lives of
402 the country's, state's, or local government's residents.

403 b. Level 4 is a severe-level incident that is likely to
404 result in a significant impact in the affected jurisdiction to
405 public health or safety; national, state, or local security;
406 economic security; or civil liberties.

576-02763A-23

20232508pb

407 c. Level 3 is a high-level incident that is likely to
408 result in a demonstrable impact in the affected jurisdiction to
409 public health or safety; national, state, or local security;
410 economic security; civil liberties; or public confidence.

411 d. Level 2 is a medium-level incident that may impact
412 public health or safety; national, state, or local security;
413 economic security; civil liberties; or public confidence.

414 e. Level 1 is a low-level incident that is unlikely to
415 impact public health or safety; national, state, or local
416 security; economic security; civil liberties; or public
417 confidence.

418 2. The cybersecurity incident reporting process must
419 specify the information that must be reported by a state agency
420 following a cybersecurity incident or ransomware incident, which
421 information must, at a minimum, include all of the following:

422 a. A summary of the facts surrounding the cybersecurity
423 incident or ransomware incident.

424 b. The date on which the state agency most recently backed
425 up its data; the physical location of the backup, if the backup
426 was affected; and whether the backup was created using cloud
427 computing.

428 c. The types of data compromised by the cybersecurity
429 incident or ransomware incident.

430 d. The estimated fiscal impact of the cybersecurity
431 incident or ransomware incident.

432 e. In the case of a ransomware incident, the details of the
433 ransom demanded.

434 3.a. A state agency shall report all ransomware incidents
435 and any cybersecurity incident determined by the state agency to

576-02763A-23

20232508pb

436 be of severity level 3, 4, or 5 to the Cybersecurity Operations
437 Center, the Cybercrime Office within the Department of Law
438 Enforcement, and the Florida Digital Service as soon as possible
439 but no later than 48 hours after discovery of the cybersecurity
440 incident and no later than 12 hours after discovery of the
441 ransomware incident. The report must contain the information
442 required to be reported under subparagraph 2.

443 b. The Cybersecurity Operations Center shall notify the
444 President of the Senate and the Speaker of the House of
445 Representatives of any severity level 3, 4, or 5 incident as
446 soon as possible but no later than 12 hours after receiving a
447 state agency's incident report. The notification must include a
448 high-level description of the incident and the likely effects.

449 4. A state agency shall report a cybersecurity incident
450 determined by the state agency to be of severity level 1 or 2 to
451 the Cybersecurity Operations Center, the Cybercrime Office
452 within the Florida Department of Law Enforcement, and the
453 Florida Digital Service as soon as possible. The report must
454 contain the information required to be reported under
455 subparagraph 2.

456 5. The Florida Digital Service shall provide a consolidated
457 incident report on a quarterly basis to the President of the
458 Senate, the Speaker of the House of Representatives, the state
459 chief information security officer, and the Florida
460 Cybersecurity Advisory Council. The report provided to the
461 Florida Cybersecurity Advisory Council may not contain the name
462 of any agency, network information, or system identifying
463 information, but must contain sufficient relevant information to
464 allow the Florida Cybersecurity Advisory Council to fulfill its

576-02763A-23

20232508pb

465 responsibilities as required in s. 282.319(9).

466 (6)~~(4)~~ Each state agency head shall, at a minimum:

467 (a) Designate an information security manager to administer
468 the cybersecurity program of the state agency. This designation
469 must be provided annually in writing to the department by
470 January 1. A state agency's information security manager, for
471 purposes of these information security duties, shall report
472 directly to the agency head.

473 (b) In consultation with the Cybersecurity Operations
474 Center ~~department, through the Florida Digital Service,~~ and the
475 Cybercrime Office within ~~of~~ the Department of Law Enforcement
476 and the Florida Digital Service within the Department of
477 Management Services, establish an agency cybersecurity response
478 team to respond to a cybersecurity incident. The agency
479 cybersecurity response team shall convene upon notification of a
480 cybersecurity incident and must immediately report all confirmed
481 or suspected incidents to the state chief information security
482 officer, or his or her designee, and comply with all applicable
483 guidelines and processes established pursuant to paragraph
484 (5) (g) ~~(3) (e)~~.

485 (c) Submit to the department annually by July 31, the state
486 agency's strategic and operational cybersecurity plans developed
487 pursuant to rules and guidelines established by the department,
488 through the Florida Digital Service.

489 1. The state agency strategic cybersecurity plan must cover
490 a 3-year period and, at a minimum, define security goals,
491 intermediate objectives, and projected agency costs for the
492 strategic issues of agency information security policy, risk
493 management, security training, security incident response, and

576-02763A-23

20232508pb

494 disaster recovery. The plan must be based on the statewide
495 cybersecurity strategic plan created by the Department of Law
496 Enforcement and include performance metrics that can be
497 objectively measured to reflect the status of the state agency's
498 progress in meeting security goals and objectives identified in
499 the agency's strategic information security plan.

500 2. The state agency operational cybersecurity plan must
501 include a progress report that objectively measures progress
502 made towards the prior operational cybersecurity plan and a
503 project plan that includes activities, timelines, and
504 deliverables for security objectives that the state agency will
505 implement during the current fiscal year.

506 3. State agencies must submit a corrective action plan for
507 all findings confirmed by the state chief information security
508 officer to the Florida Digital Service within 90 days after
509 notifications. Implementation plans that report the status of
510 the corrective action plans must be submitted on a quarterly
511 basis to the state chief information officer until fully
512 implemented.

513 (d) Annually ~~conduct, and update every 3 years,~~ a
514 comprehensive risk assessment, which may be completed by a
515 private sector vendor, to determine the security threats to the
516 data, information, and information technology resources,
517 including mobile devices and print environments, of the agency.
518 The risk assessment must comply with the risk assessment
519 methodology developed by the department and is confidential and
520 exempt from s. 119.07(1), except that such information must
521 ~~shall~~ be available to the Auditor General, the Florida Digital
522 Service within the department, the Cybercrime Office and the

576-02763A-23

20232508pb

523 Cybersecurity Operations Center within ~~of~~ the Department of Law
524 Enforcement, and, for state agencies under the jurisdiction of
525 the Governor, the Chief Inspector General. If a private sector
526 vendor is used to complete a comprehensive risk assessment, it
527 must attest to the validity of the risk assessment findings.

528 (e) Develop, and periodically update, written internal
529 policies and procedures, which include procedures for reporting
530 cybersecurity incidents and breaches to the Cybercrime Office
531 and the Cybersecurity Operations Center within ~~of~~ the Department
532 of Law Enforcement and the Florida Digital Service within the
533 department. Such policies and procedures must be consistent with
534 the rules, guidelines, and processes established by the
535 department to ensure the security of the data, information, and
536 information technology resources of the agency. The internal
537 policies and procedures that, if disclosed, could facilitate the
538 unauthorized modification, disclosure, or destruction of data or
539 information technology resources are confidential information
540 and exempt from s. 119.07(1), except that such information must
541 ~~shall~~ be available to the Auditor General, the Cybercrime Office
542 and the Cybersecurity Operations Center within ~~of~~ the Department
543 of Law Enforcement, the Florida Digital Service within the
544 department, and, for state agencies under the jurisdiction of
545 the Governor, the Chief Inspector General.

546 (f) Implement managerial, operational, and technical
547 safeguards and risk assessment remediation plans recommended by
548 the department to address identified risks to the data,
549 information, and information technology resources of the agency.
550 The department, through the Florida Digital Service, shall track
551 implementation by state agencies upon development of such

576-02763A-23

20232508pb

552 remediation plans in coordination with agency inspectors
553 general.

554 (g) Ensure that periodic internal audits and evaluations of
555 the agency's cybersecurity program for the data, information,
556 and information technology resources of the agency are
557 conducted. The results of such audits and evaluations are
558 confidential information and exempt from s. 119.07(1), except
559 that such information must ~~shall~~ be available to the Auditor
560 General, the Cybercrime Office and the Cybersecurity Operations
561 Center within ~~of~~ the Department of Law Enforcement, the Florida
562 Digital Service within the department, and, for agencies under
563 the jurisdiction of the Governor, the Chief Inspector General.

564 (h) Ensure that the cybersecurity requirements in the
565 written specifications for the solicitation, contracts, and
566 service-level agreement of information technology and
567 information technology resources and services meet or exceed the
568 applicable state and federal laws, regulations, and standards
569 for cybersecurity, including the National Institute of Standards
570 and Technology Cybersecurity Framework. Service-level agreements
571 must identify service provider and state agency responsibilities
572 for privacy and security, protection of government data,
573 personnel background screening, and security deliverables with
574 associated frequencies.

575 (i) Provide cybersecurity awareness training to all state
576 agency employees within 30 days after commencing employment, and
577 annually thereafter, concerning cybersecurity risks and the
578 responsibility of employees to comply with policies, standards,
579 guidelines, and operating procedures adopted by the state agency
580 to reduce those risks. The training may be provided in

576-02763A-23

20232508pb

581 collaboration with the Cybercrime Office and the Cybersecurity
582 Operations Center within ~~of~~ the Department of Law Enforcement,
583 the Florida Digital Service, a private sector entity, or an
584 institution of the State University System.

585 (j) Develop a process for detecting, reporting, and
586 responding to threats, breaches, or cybersecurity incidents
587 which is consistent with the security rules, guidelines, and
588 processes established by the Department of Law Enforcement
589 ~~through the Florida Digital Service~~.

590 1. All cybersecurity incidents and ransomware incidents
591 must be reported by state agencies. Such reports must comply
592 with the notification procedures and reporting timeframes
593 established pursuant to paragraph (5) (g) ~~(3) (e)~~.

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

596 (k) Submit to the Department of Law Enforcement and the
597 Florida Digital Service, within 1 week after the remediation of
598 a cybersecurity incident or ransomware incident, an after-action
599 report that summarizes the incident, the incident's resolution,
600 and any insights gained as a result of the incident.

601 (7) (5) The portions of risk assessments, evaluations,
602 external audits, and other reports of a state agency's
603 cybersecurity program for the data, information, and information
604 technology resources of the state agency which are held by a
605 state agency are confidential and exempt from s. 119.07(1) and
606 s. 24(a), Art. I of the State Constitution if the disclosure of
607 such portions of records would facilitate unauthorized access to
608 or the unauthorized modification, disclosure, or destruction of:

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

576-02763A-23

20232508pb

- 610 (b) Information technology resources, which include:
- 611 1. Information relating to the security of the agency's
- 612 technologies, processes, and practices designed to protect
- 613 networks, computers, data processing software, and data from
- 614 attack, damage, or unauthorized access; or
- 615 2. Security information, whether physical or virtual, which
- 616 relates to the agency's existing or proposed information
- 617 technology systems.

618

619 For purposes of this subsection, "external audit" means an audit

620 that is conducted by an entity other than the state agency that

621 is the subject of the audit.

622 (8)~~(6)~~ Those portions of a public meeting as specified in

623 s. 286.011 which would reveal records which are confidential and

624 exempt under subsection (7) ~~(5)~~ are exempt from s. 286.011 and

625 s. 24(b), Art. I of the State Constitution. No exempt portion of

626 an exempt meeting may be off the record. All exempt portions of

627 such meeting must ~~shall~~ be recorded and transcribed. Such

628 recordings and transcripts are confidential and exempt from

629 disclosure under s. 119.07(1) and s. 24(a), Art. I of the State

630 Constitution unless a court of competent jurisdiction, after an

631 in camera review, determines that the meeting was not restricted

632 to the discussion of data and information made confidential and

633 exempt by this section. In the event of such a judicial

634 determination, only that portion of the recording and transcript

635 which reveals nonexempt data and information may be disclosed to

636 a third party.

637 (9)~~(7)~~ The portions of records made confidential and exempt

638 in subsections (7) ~~(5)~~ and (8) must ~~(6)~~ ~~shall~~ be available to

576-02763A-23

20232508pb

639 the Auditor General, the Cybercrime Office and the state chief
640 information officer within ~~of~~ the Department of Law Enforcement,
641 the Florida Digital Service within the department, and, for
642 agencies under the jurisdiction of the Governor, the Chief
643 Inspector General. Such portions of records may be made
644 available to a local government, another state agency, or a
645 federal agency for cybersecurity purposes or in furtherance of
646 the state agency's official duties.

647 (10)~~(8)~~ The exemptions contained in subsections (7) ~~(5)~~ and
648 (8) ~~(6)~~ apply to records held by a state agency before, on, or
649 after the effective date of this exemption.

650 (11)~~(9)~~ Subsections (7) ~~(5)~~ and (8) ~~(6)~~ are subject to the
651 Open Government Sunset Review Act in accordance with s. 119.15
652 and shall stand repealed on October 2, 2025, unless reviewed and
653 saved from repeal through reenactment by the Legislature.

654 (12)~~(10)~~ The department and the Department of Law
655 Enforcement shall adopt rules relating to cybersecurity and to
656 administer this section.

657 Section 3. Section 282.3185, Florida Statutes, is amended
658 to read:

659 282.3185 Local government cybersecurity.—

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

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

664 (3) CYBERSECURITY TRAINING.—

665 (a) The Florida Digital Service shall:

666 1. Develop a basic cybersecurity training curriculum for
667 local government employees which must be approved by the state

576-02763A-23

20232508pb

668 chief information security officer. All local government
669 employees with access to the local government's network must
670 complete the basic cybersecurity training within 30 days after
671 commencing employment and annually thereafter.

672 2. Develop an advanced cybersecurity training curriculum
673 for local governments which is consistent with the cybersecurity
674 training required under s. 282.318(3)(e) and which must be
675 approved by the state chief information security officer ~~s.~~
676 ~~282.318(3)(g)~~. All local government technology professionals and
677 employees with access to highly sensitive information must
678 complete the advanced cybersecurity training within 30 days
679 after commencing employment and annually thereafter.

680 (b) The Florida Digital Service may provide the
681 cybersecurity training required by this subsection in
682 collaboration with the Cybercrime Office and the Cybersecurity
683 Operations Center within ~~of~~ the Department of Law Enforcement, a
684 private sector entity, or an institution of the State University
685 System.

686 (4) CYBERSECURITY STANDARDS.—

687 (a) Each local government shall adopt cybersecurity
688 standards that safeguard its data, information technology, and
689 information technology resources to ensure availability,
690 confidentiality, and integrity. The cybersecurity standards must
691 be consistent with generally accepted best practices for
692 cybersecurity, including the National Institute of Standards and
693 Technology Cybersecurity Framework.

694 (b) Each county with a population of 75,000 or more must
695 adopt the cybersecurity standards required by this subsection by
696 January 1, 2024. Each county with a population of less than

576-02763A-23

20232508pb

697 75,000 must adopt the cybersecurity standards required by this
698 subsection by January 1, 2025.

699 (c) Each municipality with a population of 25,000 or more
700 must adopt the cybersecurity standards required by this
701 subsection by January 1, 2024. Each municipality with a
702 population of less than 25,000 must adopt the cybersecurity
703 standards required by this subsection by January 1, 2025.

704 (d) Each local government shall notify the Florida Digital
705 Service of its compliance with this subsection as soon as
706 possible.

707 (5) INCIDENT NOTIFICATION.—

708 (a) A local government shall provide notification of a
709 cybersecurity incident or ransomware incident to the
710 Cybersecurity Operations Center and the Cybercrime Office
711 within ~~of~~ the Department of Law Enforcement, the Florida Digital
712 Service, and the sheriff who has jurisdiction over the local
713 government in accordance with paragraph (b). The notification
714 must include, at a minimum, the following information:

715 1. A summary of the facts surrounding the cybersecurity
716 incident or ransomware incident.

717 2. The date on which the local government most recently
718 backed up its data; the physical location of the backup, if the
719 backup was affected; and if the backup was created using cloud
720 computing.

721 3. The types of data compromised by the cybersecurity
722 incident or ransomware incident.

723 4. The estimated fiscal impact of the cybersecurity
724 incident or ransomware incident.

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

576-02763A-23

20232508pb

726 ransom demanded.

727 6. A statement requesting or declining assistance from the
728 Cybersecurity Operations Center and, the Cybercrime Office
729 within ~~of~~ the Department of Law Enforcement, the Florida Digital
730 Service, or the sheriff who has jurisdiction over the local
731 government.

732 (b)1. A local government shall report all ransomware
733 incidents and any cybersecurity incident determined by the local
734 government to be of severity level 3, 4, or 5 as provided in s.
735 282.318(5)(g) ~~s. 282.318(3)(e)~~ to the Cybersecurity Operations
736 Center and, the Cybercrime Office within ~~of~~ the Department of
737 Law Enforcement, the Florida Digital Service, and the sheriff
738 who has jurisdiction over the local government as soon as
739 possible but no later than 48 hours after discovery of the
740 cybersecurity incident and no later than 12 hours after
741 discovery of the ransomware incident. The report must contain
742 the information required in paragraph (a).

743 2. The Cybersecurity Operations Center shall notify the
744 President of the Senate and the Speaker of the House of
745 Representatives of any severity level 3, 4, or 5 incident as
746 soon as possible but no later than 12 hours after receiving a
747 local government's incident report. The notification must
748 include a high-level description of the incident and the likely
749 effects.

750 (c) A local government may report a cybersecurity incident
751 determined by the local government to be of severity level 1 or
752 2 as provided in s. 282.318(5)(g) ~~s. 282.318(3)(e)~~ to the
753 Cybersecurity Operations Center and, the Cybercrime Office
754 within ~~of~~ the Department of Law Enforcement, the Florida Digital

576-02763A-23

20232508pb

755 Service, and the sheriff who has jurisdiction over the local
756 government. The report must ~~shall~~ contain the information
757 required in paragraph (a).

758 (d) The Florida Digital Service ~~Cybersecurity Operations~~
759 ~~Center~~ shall provide a consolidated incident report on a
760 quarterly basis to the President of the Senate, the Speaker of
761 the House of Representatives, the state chief information
762 security officer, and the Florida Cybersecurity Advisory
763 Council. The report provided to the Florida Cybersecurity
764 Advisory Council may not contain the name of any local
765 government, network information, or system identifying
766 information but must contain sufficient relevant information to
767 allow the Florida Cybersecurity Advisory Council to fulfill its
768 responsibilities as required in s. 282.319(9).

769 (6) AFTER-ACTION REPORT.—A local government must submit to
770 the Cybersecurity Operations Center and the Florida Digital
771 Service, within 1 week after the remediation of a cybersecurity
772 incident or ransomware incident, an after-action report that
773 summarizes the incident, the incident's resolution, and any
774 insights gained as a result of the incident. By December 1, 2023
775 ~~2022~~, the Florida Digital Service shall collaborate with the
776 state chief information security officer to establish guidelines
777 and processes for submitting an after-action report.

778 Section 4. This act shall take effect July 1, 2023.