

ENROLLED

CS/HB 7055

2022 Legislature

1  
 2 An act relating to cybersecurity; amending s.  
 3 282.0041, F.S.; providing and revising definitions;  
 4 amending s. 282.318, F.S.; requiring the Department of  
 5 Management Services, acting through the Florida  
 6 Digital Service, to develop and publish guidelines and  
 7 processes for reporting cybersecurity incidents;  
 8 requiring state agencies to report ransomware  
 9 incidents and certain cybersecurity incidents to  
 10 certain entities within specified timeframes;  
 11 requiring the Cybersecurity Operations Center to  
 12 provide certain notifications to the Legislature  
 13 within a specified timeframe; requiring the  
 14 Cybersecurity Operations Center to quarterly provide  
 15 certain reports to the Legislature and the Florida  
 16 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

ENROLLED

CS/HB 7055

2022 Legislature

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; providing a  
30 | definition; requiring the Florida Digital Service to  
31 | develop certain cybersecurity training curricula;  
32 | requiring certain persons to complete certain  
33 | cybersecurity training within a specified timeframe  
34 | and annually thereafter; authorizing the Florida  
35 | Digital Service to provide certain training in  
36 | collaboration with certain entities; requiring certain  
37 | local governments to adopt certain cybersecurity  
38 | standards by specified dates; requiring local  
39 | governments to provide certain notification to the  
40 | 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 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

ENROLLED

CS/HB 7055

2022 Legislature

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;  
 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 providing a definition; creating s. 815.062, F.S.;  
 69 providing a definition; providing criminal penalties;  
 70 requiring a person convicted of certain offenses to  
 71 pay a certain fine; requiring deposit of certain  
 72 moneys in the General Revenue Fund; providing a  
 73 legislative finding and declaration of an important  
 74 state interest; providing an effective date.

75

ENROLLED

CS/HB 7055

2022 Legislature

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

77

78 Section 1. Subsections (28) through (37) of section  
 79 282.0041, Florida Statutes, are renumbered as subsections (29)  
 80 through (38), respectively, subsection (19) is amended, and a  
 81 new subsection (28) is added to that section, to read:

82 282.0041 Definitions.—As used in this chapter, the term:

83 (19) "Incident" means a violation or imminent threat of  
 84 violation, whether such violation is accidental or deliberate,  
 85 of information technology resources, security, policies, or  
 86 practices. An imminent threat of violation refers to a situation  
 87 in which a the state agency, county, or municipality has a  
 88 factual basis for believing that a specific incident is about to  
 89 occur.

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

97 Section 2. Paragraphs (c) and (g) of subsection (3) and  
 98 paragraphs (i) and (j) of subsection (4) of section 282.318,  
 99 Florida Statutes, are amended, and paragraph (k) is added to  
 100 subsection (4) of that section, to read:

ENROLLED

CS/HB 7055

2022 Legislature

101 282.318 Cybersecurity.—

102 (3) The department, acting through the Florida Digital  
 103 Service, is the lead entity responsible for establishing  
 104 standards and processes for assessing state agency cybersecurity  
 105 risks and determining appropriate security measures. Such  
 106 standards and processes must be consistent with generally  
 107 accepted technology best practices, including the National  
 108 Institute for Standards and Technology Cybersecurity Framework,  
 109 for cybersecurity. The department, acting through the Florida  
 110 Digital Service, shall adopt rules that mitigate risks;  
 111 safeguard state agency digital assets, data, information, and  
 112 information technology resources to ensure availability,  
 113 confidentiality, and integrity; and support a security  
 114 governance framework. The department, acting through the Florida  
 115 Digital Service, shall also:

116 (c) Develop and publish for use by state agencies a  
 117 cybersecurity governance framework that, at a minimum, includes  
 118 guidelines and processes for:

119 1. Establishing asset management procedures to ensure that  
 120 an agency's information technology resources are identified and  
 121 managed consistent with their relative importance to the  
 122 agency's business objectives.

123 2. Using a standard risk assessment methodology that  
 124 includes the identification of an agency's priorities,  
 125 constraints, risk tolerances, and assumptions necessary to

ENROLLED

CS/HB 7055

2022 Legislature

126 support operational risk decisions.

127         3. Completing comprehensive risk assessments and  
 128 cybersecurity audits, which may be completed by a private sector  
 129 vendor, and submitting completed assessments and audits to the  
 130 department.

131         4. Identifying protection procedures to manage the  
 132 protection of an agency's information, data, and information  
 133 technology resources.

134         5. Establishing procedures for accessing information and  
 135 data to ensure the confidentiality, integrity, and availability  
 136 of such information and data.

137         6. Detecting threats through proactive monitoring of  
 138 events, continuous security monitoring, and defined detection  
 139 processes.

140         7. Establishing agency cybersecurity incident response  
 141 teams and describing their responsibilities for responding to  
 142 cybersecurity incidents, including breaches of personal  
 143 information containing confidential or exempt data.

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

147         9. Establishing a cybersecurity incident reporting process  
 148 that includes procedures ~~and tiered reporting timeframes~~ for  
 149 notifying the department and the Department of Law Enforcement  
 150 of cybersecurity incidents. ~~The tiered reporting timeframes~~

ENROLLED

CS/HB 7055

2022 Legislature

151 ~~shall be based upon the level of severity of the cybersecurity~~  
 152 ~~incidents being reported.~~

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

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

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

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

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

172 (V) Level 1 is a low-level incident that is unlikely to  
 173 impact public health or safety; national, state, or local  
 174 security; economic security; civil liberties; or public  
 175 confidence.

ENROLLED

CS/HB 7055

2022 Legislature

176 b. The cybersecurity incident reporting process must  
 177 specify the information that must be reported by a state agency  
 178 following a cybersecurity incident or ransomware incident,  
 179 which, at a minimum, must include the following:

180 (I) A summary of the facts surrounding the cybersecurity  
 181 incident or ransomware incident.

182 (II) The date on which the state agency most recently  
 183 backed up its data, the physical location of the backup, if the  
 184 backup was affected, and if the backup was created using cloud  
 185 computing.

186 (III) The types of data compromised by the cybersecurity  
 187 incident or ransomware incident.

188 (IV) The estimated fiscal impact of the cybersecurity  
 189 incident or ransomware incident.

190 (V) In the case of a ransomware incident, the details of  
 191 the ransom demanded.

192 c.(I) A state agency shall report all ransomware incidents  
 193 and any cybersecurity incident determined by the state agency to  
 194 be of severity level 3, 4, or 5 to the Cybersecurity Operations  
 195 Center and the Cybercrime Office of the Department of Law  
 196 Enforcement as soon as possible but no later than 48 hours after  
 197 discovery of the cybersecurity incident and no later than 12  
 198 hours after discovery of the ransomware incident. The report  
 199 must contain the information required in sub-subparagraph b.

200 (II) The Cybersecurity Operations Center shall notify the



ENROLLED

CS/HB 7055

2022 Legislature

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

206 d. A state agency shall report a cybersecurity incident  
 207 determined by the state agency to be of severity level 1 or 2 to  
 208 the Cybersecurity Operations Center and the Cybercrime Office of  
 209 the Department of Law Enforcement as soon as possible. The  
 210 report must contain the information required in sub-subparagraph  
 211 b.

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

222 10. Incorporating information obtained through detection  
 223 and response activities into the agency's cybersecurity incident  
 224 response plans.

225 11. Developing agency strategic and operational

ENROLLED

CS/HB 7055

2022 Legislature

226 cybersecurity plans required pursuant to this section.

227 12. Establishing the managerial, operational, and  
 228 technical safeguards for protecting state government data and  
 229 information technology resources that align with the state  
 230 agency risk management strategy and that protect the  
 231 confidentiality, integrity, and availability of information and  
 232 data.

233 13. Establishing procedures for procuring information  
 234 technology commodities and services that require the commodity  
 235 or service to meet the National Institute of Standards and  
 236 Technology Cybersecurity Framework.

237 14. Submitting after-action reports following a  
 238 cybersecurity incident or ransomware incident. Such guidelines  
 239 and processes for submitting after-action reports must be  
 240 developed and published by December 1, 2022.

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

ENROLLED

CS/HB 7055

2022 Legislature

251 (4) Each state agency head shall, at a minimum:  
 252 (i) Provide cybersecurity awareness training to all state  
 253 agency employees within ~~in the first~~ 30 days after commencing  
 254 employment, and annually thereafter, concerning cybersecurity  
 255 risks and the responsibility of employees to comply with  
 256 policies, standards, guidelines, and operating procedures  
 257 adopted by the state agency to reduce those risks. The training  
 258 may be provided in collaboration with the Cybercrime Office of  
 259 the Department of Law Enforcement, a private sector entity, or  
 260 an institution of the State University System.

261 (j) Develop a process for detecting, reporting, and  
 262 responding to threats, breaches, or cybersecurity incidents  
 263 which is consistent with the security rules, guidelines, and  
 264 processes established by the department through the Florida  
 265 Digital Service.

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

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

274 (k) Submit to the Florida Digital Service, within 1 week  
 275 after the remediation of a cybersecurity incident or ransomware

ENROLLED

CS/HB 7055

2022 Legislature

276 incident, an after-action report that summarizes the incident,  
 277 the incident's resolution, and any insights gained as a result  
 278 of the incident.

279 Section 3. Section 282.3185, Florida Statutes, is created  
 280 to read:

281 282.3185 Local government cybersecurity.-

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

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

286 (3) CYBERSECURITY TRAINING.-

287 (a) The Florida Digital Service shall:

288 1. Develop a basic cybersecurity training curriculum for  
 289 local government employees. All local government employees with  
 290 access to the local government's network must complete the basic  
 291 cybersecurity training within 30 days after commencing  
 292 employment and annually thereafter.

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

300 (b) The Florida Digital Service may provide the

ENROLLED

CS/HB 7055

2022 Legislature

301 cybersecurity training required by this subsection in  
302 collaboration with the Cybercrime Office of the Department of  
303 Law Enforcement, a private sector entity, or an institution of  
304 the State University System.

305 (4) CYBERSECURITY STANDARDS.—

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

313 (b) Each county with a population of 75,000 or more must  
314 adopt the cybersecurity standards required by this subsection by  
315 January 1, 2024. Each county with a population of less than  
316 75,000 must adopt the cybersecurity standards required by this  
317 subsection by January 1, 2025.

318 (c) Each municipality with a population of 25,000 or more  
319 must adopt the cybersecurity standards required by this  
320 subsection by January 1, 2024. Each municipality with a  
321 population of less than 25,000 must adopt the cybersecurity  
322 standards required by this subsection by January 1, 2025.

323 (d) Each local government shall notify the Florida Digital  
324 Service of its compliance with this subsection as soon as  
325 possible.

ENROLLED

CS/HB 7055

2022 Legislature

326       (5) INCIDENT NOTIFICATION.—  
 327       (a) A local government shall provide notification of a  
 328 cybersecurity incident or ransomware incident to the  
 329 Cybersecurity Operations Center, Cybercrime Office of the  
 330 Department of Law Enforcement, and sheriff who has jurisdiction  
 331 over the local government in accordance with paragraph (b). The  
 332 notification must include, at a minimum, the following  
 333 information:  
 334       1. A summary of the facts surrounding the cybersecurity  
 335 incident or ransomware incident.  
 336       2. The date on which the local government most recently  
 337 backed up its data, the physical location of the backup, if the  
 338 backup was affected, and if the backup was created using cloud  
 339 computing.  
 340       3. The types of data compromised by the cybersecurity  
 341 incident or ransomware incident.  
 342       4. The estimated fiscal impact of the cybersecurity  
 343 incident or ransomware incident.  
 344       5. In the case of a ransomware incident, the details of  
 345 the ransom demanded.  
 346       6. A statement requesting or declining assistance from the  
 347 Cybersecurity Operations Center, the Cybercrime Office of the  
 348 Department of Law Enforcement, or the sheriff who has  
 349 jurisdiction over the local government.  
 350       (b)1. A local government shall report all ransomware

ENROLLED

CS/HB 7055

2022 Legislature

351 incidents and any cybersecurity incident determined by the local  
 352 government to be of severity level 3, 4, or 5 as provided in s.  
 353 282.318(3)(c) to the Cybersecurity Operations Center, the  
 354 Cybercrime Office of the Department of Law Enforcement, and the  
 355 sheriff who has jurisdiction over the local government as soon  
 356 as possible but no later than 48 hours after discovery of the  
 357 cybersecurity incident and no later than 12 hours after  
 358 discovery of the ransomware incident. The report must contain  
 359 the information required in paragraph (a).

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

367 (c) A local government may report a cybersecurity incident  
 368 determined by the local government to be of severity level 1 or  
 369 2 as provided in s. 282.318(3)(c) to the Cybersecurity  
 370 Operations Center, the Cybercrime Office of the Department of  
 371 Law Enforcement, and the sheriff who has jurisdiction over the  
 372 local government. The report shall contain the information  
 373 required in paragraph (a).

374 (d) The Cybersecurity Operations Center shall provide a  
 375 consolidated incident report on a quarterly basis to the

ENROLLED

CS/HB 7055

2022 Legislature

376 President of the Senate, the Speaker of the House of  
377 Representatives, and the Florida Cybersecurity Advisory Council.  
378 The report provided to the Florida Cybersecurity Advisory  
379 Council may not contain the name of any local government,  
380 network information, or system identifying information but must  
381 contain sufficient relevant information to allow the Florida  
382 Cybersecurity Advisory Council to fulfill its responsibilities  
383 as required in s. 282.319(9).

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

391 Section 4. Section 282.3186, Florida Statutes, is created  
392 to read:

393 282.3186 Ransomware incident compliance.—A state agency as  
394 defined in s. 282.318(2), a county, or a municipality  
395 experiencing a ransomware incident may not pay or otherwise  
396 comply with a ransom demand.

397 Section 5. Subsections (2) of section 282.319, Florida  
398 Statutes, is amended, paragraphs (g) and (h) are added to  
399 subsection (9), and subsections (12) and (13) are added to that  
400 section, to read:



ENROLLED

CS/HB 7055

2022 Legislature

401           282.319 Florida Cybersecurity Advisory Council.—

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

403           (a) Assist state agencies in protecting their information

404 technology resources from ~~cybersecurity~~ ~~cyber~~ threats and

405 incidents.

406           (b) Advise counties and municipalities on cybersecurity,

407 including cybersecurity threats, trends, and best practices.

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

409           (g) Review information relating to cybersecurity incidents

410 and ransomware incidents to determine commonalities and develop

411 best practice recommendations for state agencies, counties, and

412 municipalities.

413           (h) Recommend any additional information that a county or

414 municipality should report to the Florida Digital Service as

415 part of its cybersecurity incident or ransomware incident

416 notification pursuant to s. 282.3185.

417           (12) Beginning December 1, 2022, and each December 1

418 thereafter, the council shall submit to the Governor, the

419 President of the Senate, and the Speaker of the House of

420 Representatives a comprehensive report that includes data,

421 trends, analysis, findings, and recommendations for state and

422 local action regarding ransomware incidents. At a minimum, the

423 report must include:

424           (a) Descriptive statistics including the amount of ransom

425 requested, duration of the ransomware incident, and overall

ENROLLED

CS/HB 7055

2022 Legislature

426 monetary cost to taxpayers of the ransomware incident.

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

431 (c) A detailed statistical analysis of the level of  
 432 cybersecurity employee training and frequency of data backup for  
 433 the state agency, county, or municipality that reported the  
 434 ransomware incident.

435 (d) Specific issues identified with current policies,  
 436 procedures, rules, or statutes and recommendations to address  
 437 such issues.

438 (e) Any other recommendations to prevent ransomware  
 439 incidents.

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

442 Section 6. Section 815.062, Florida Statutes, is created  
 443 to read:

444 815.062 Offenses against governmental entities.—

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

ENROLLED

CS/HB 7055

2022 Legislature

451 state.

452 (2) A person who willfully, knowingly, and without  
 453 authorization introduces a computer contaminant that gains  
 454 unauthorized access to, encrypts, modifies, or otherwise renders  
 455 unavailable data, programs, or supporting documentation residing  
 456 or existing within a computer, computer system, computer  
 457 network, or electronic device owned or operated by a  
 458 governmental entity and demands a ransom to prevent the  
 459 publication of or restore access to the data, programs, or  
 460 supporting documentation or to otherwise remediate the impact of  
 461 the computer contaminant commits a felony of the first degree,  
 462 punishable as provided in s. 775.082, s. 775.083, or s. 775.084.

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

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

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

ENROLLED

CS/HB 7055

2022 Legislature

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