Fla. Stat. § 282.319

Current through Chapter 1 of the 2024 session and through the 2023 C special session.

LexisNexis® Florida Annotated Statutes > Title XIX. Public Business. (Chs. 279 — 290) > Chapter 282. Communications and Data Processing. (Pts. I — III) > Part I. Enterprise Information Technology Services Management. (§§ 282.003 — 282.34)

§ 282.319. Florida Cybersecurity Advisory Council.

(1) The Florida Cybersecurity Advisory Council, an advisory council as defined in s. 20.03(7), is created within the department. Except as otherwise provided in this section, the advisory council shall operate in a manner consistent with s. 20.052.

(2) The purpose of the council is to:

(a) Assist state agencies in protecting their information technology resources from cybersecurity threats and incidents.

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

(3) The council shall assist the Florida Digital Service in implementing best cybersecurity practices, taking into consideration the final recommendations of the Florida Cybersecurity Task Force created under chapter 2019-118, Laws of Florida.

(4) The council shall be comprised of the following members:

(a) The Lieutenant Governor or his or her designee.

(b) The state chief information officer.

(c) The state chief information security officer.

(d) The director of the Division of Emergency Management or his or her designee.

(e) A representative of the computer crime center of the Department of Law Enforcement, appointed by the executive director of the Department of Law Enforcement.

(f) A representative of the Florida Fusion Center of the Department of Law Enforcement, appointed by the executive director of the Department of Law Enforcement.

(g) The Chief Inspector General.

(h) A representative from the Public Service Commission.

(i) Up to two representatives from institutions of higher education located in this state, appointed by the Governor.

(j) Three representatives from critical infrastructure sectors, one of whom must be from a water treatment facility, appointed by the Governor.

(k) Four representatives of the private sector with senior level experience in cybersecurity or software engineering from within the finance, energy, health care, and transportation sectors, appointed by the Governor.

(l) Two representatives with expertise on emerging technology, with one appointed by the President of the Senate and one appointed by the Speaker of the House of Representatives.

(5) Members shall serve for a term of 4 years; however, for the purpose of providing staggered terms, the initial appointments of members made by the Governor shall be for a term of 2 years. A vacancy shall be filled for the remainder of the unexpired term in the same manner as the initial appointment. All members of the council are eligible for reappointment.

(6) The Secretary of Management Services, or his or her designee, shall serve as the ex officio, nonvoting executive director of the council.

(7) Members of the council shall serve without compensation but are entitled to receive reimbursement for per diem and travel expenses pursuant to s. 112.061.

(8) Members of the council shall maintain the confidential or exempt status of information received in the performance of their duties and responsibilities as members of the council. In accordance with s. 112.313, a current or former member of the council may not disclose or use information not available to the general public and gained by reason of their official position, except for information relating exclusively to governmental practices, for their personal gain or benefit or for the personal gain or benefit of any other person or business entity. Members shall sign an agreement acknowledging the provisions of this subsection.

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

(a) Review existing state agency cybersecurity policies.

(b) Assess ongoing risks to state agency information technology.

(c) Recommend a reporting and information sharing system to notify state agencies of new risks.

(d) Recommend data breach simulation exercises.

(e) Assist the Florida Digital Service in developing cybersecurity best practice recommendations for state agencies that include recommendations regarding:

1. Continuous risk monitoring.

2. Password management.

3. Protecting data in legacy and new systems.

(f) Examine inconsistencies between state and federal law regarding cybersecurity.

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

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

(10) The council shall work with the National Institute of Standards and Technology and other federal agencies, private sector businesses, and private cybersecurity experts:

(a) For critical infrastructure not covered by federal law, to identify which local infrastructure sectors are at the greatest risk of cyber attacks and need the most enhanced cybersecurity measures.

(b) To use federal guidance to identify categories of critical infrastructure as critical cyber infrastructure if cyber damage or unauthorized cyber access to the infrastructure could reasonably result in catastrophic consequences.

(11) Each June 30, the council shall submit to the President of the Senate and the Speaker of the House of Representatives any legislative recommendations considered necessary by the council to address cybersecurity.

(12) Each December 1, the council shall submit to the Governor, the President of the Senate, and the Speaker of the House of Representatives a comprehensive report that includes data, trends, analysis, findings, and recommendations for state and local action regarding ransomware incidents. At a minimum, the report must include:

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

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

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

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

(e) Any other recommendations to prevent ransomware incidents.

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

History

S. 7, ch. 2021-234, effective July 1, 2021; s. 14, ch. 2022-4, effective May 13, 2022; s. 5, ch. 2022-220, effective July 1, 2022; s. 57, ch. 2023-8, effective July 1, 2023.

End of Document