

Committee on Governmental Oversight and Accountability

SB 7020 — OGSR/Agency Cybersecurity Information

by Governmental Oversight and Accountability Committee and Senator DiCeglie

The bill aligns the scheduled repeal dates for specified cybersecurity related public record and public meeting exemptions to allow for a simultaneous review. Specifically, the bill delays for one year (from October 2, 2025 to October 2, 2026) the repeal date of the exemption in s. 282.318(5), F.S., which makes confidential and exempt from public inspection and copying requirements the portions of risk assessments, evaluations, external audits, and other reports of a state agency cybersecurity program for the data, information, and state agency IT resources which are held by the state agency, if the disclosure of such portions of records would facilitate the unauthorized access to, or the unauthorized modification, disclosure, or destruction of:

- Data or information, whether physical or virtual; or
- IT resources, which include:
 - Information relating to the security of the agency's technologies, processes, and practices designed to protect networks, computers, data processing software, and data from attack, damage, or unauthorized access; or
 - Security information, whether physical or virtual, which relates to the agency's existing or proposed IT systems.

The bill also delays from repeal the current public meetings exemption for any portion of a meeting that would reveal the information described above.

The bill moves up by one year (from October 2, 2027 to October 2, 2026) the sunset review date for, and repeal of, the public record and public meeting exemption codified in s. 119.0725(2) and (3), F.S. This general cybersecurity public record and public meeting exemption makes confidential and exempt from public inspection and copying requirements the following information held by an agency before, on, or after July 1, 2022:

- Coverage limits and deductible or self-insurance amounts of insurance or other risk mitigation coverages acquired for the protection of IT systems, operational technology systems, or data of an agency.
- Information relating to critical infrastructure.
- Cybersecurity incident information that is reported by a state agency or local government pursuant to ss. 282.318 or 282.3185, F.S.
- Network schematics, hardware and software configurations, or encryption information or information that identifies detection, investigation, or response practices for suspected or confirmed cybersecurity incidents.

Any portion of a public meeting that would reveal the above confidential and exempt information is closed to the public and exempt from public meeting laws.

If approved by the Governor, or allowed to become law without the Governor's signature, these provisions take effect July 1, 2025.

Vote: Senate 37-0; House 116-0