HOUSE OF REPRESENTATIVES STAFF FINAL BILL ANALYSIS

BILL #: CS/HB 7057 PCB SAT 22-03 Pub. Rec. and Meetings/Cybersecurity
SPONSOR(S): State Affairs Committee and State Administration & Technology Appropriations Subcommittee, Giallombardo and others
TIED BILLS: CS/HB 7055 **IDEN./SIM. BILLS:** CS/CS/SB 1694

FINAL HOUSE FLOOR ACTION: 111 **Y's** 0 **N's** **GOVERNOR'S ACTION:** Approved

SUMMARY ANALYSIS

CS/HB 7057 passed the House on March 4, 2022, and subsequently passed the Senate on March 9, 2022.

Current law provides a public record and meeting exemption for certain information held by a state agency related to cybersecurity or potential breaches of security. It also provides public record exemptions related to information technology (IT) and cybersecurity information of a utility owned or operated by a unit of local government or certain cybersecurity information held by supervisors of elections. However, there is no general public record exemption or public meeting exemption related to state or local government cybersecurity information.

CS/HB 7055, to which this bill is linked, creates cybersecurity related requirements for state agencies and local governments. It requires state agencies and local governments to report ransomware incidents and high severity level cybersecurity incidents and requires local governments to adopt cybersecurity standards that safeguard the local government's data, IT, and IT resources by a date certain.

The bill provides a general public record exemption in ch. 119, F.S., for 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.
- Network schematics, hardware and software configurations, or encryption information or information that identifies detection, investigation, or response practices for suspected or confirmed cybersecurity incidents.
- Cybersecurity incident information reported pursuant to Sections 282.318 or 282.3185, F.S.

The bill also creates a public meeting exemption for any portion of a meeting that would reveal the confidential and exempt information; however, any portion of an exempt meeting must be recorded and transcribed. The recording and transcript are confidential and exempt from public record requirements.

The bill provides for release of the confidential and exempt information in certain instances and authorizes agencies to report information about cybersecurity incidents in an aggregate format.

The bill provides for repeal of the exemptions on October 2, 2027, unless reviewed and saved from repeal by the Legislature, and provides a public necessity statement as required by the Florida Constitution.

The bill may have a minimal fiscal impact on the state and local governments. *See* Fiscal Comments.

This bill was approved by the Governor on June 24, 2022, ch. 2022-221, L.O.F., and will become effective on the same date that CS/HB 7055 (2022) takes effect.

I. SUBSTANTIVE INFORMATION

A. EFFECT OF CHANGES:

Background

Public Records
Article I, s. 24(a) of the Florida Constitution sets forth the state's public policy regarding access to government records. This section guarantees every person a right to inspect or copy any public record of the legislative, executive, and judicial branches of government.

Public policy regarding access to government records is addressed further in s. 119.07(1)(a), F.S., which guarantees every person a right to inspect and copy any state, county, or municipal record, unless the record is exempt.

Public Meetings
Article I, s. 24(b) of the Florida Constitution requires all meetings of any collegial public body of the executive branch of state government or any collegial public body of a county, municipality, school district, or special district, at which official acts are to be taken or at which public business of such body is to be transacted or discussed, be open and noticed to the public.

Public policy regarding access to government meetings also is addressed in the Florida Statutes. Section 286.011, F.S., known as the "Government in the Sunshine Law" or "Sunshine Law," further requires all meetings of any board or commission of any state agency or authority, or of any agency or authority of any county, municipality, or political subdivision, at which official acts are to be taken to be open to the public at all times.[1] The board or commission must provide reasonable notice of all public meetings.[2] Public meetings may not be held at any location that discriminates on the basis of sex, age, race, creed, color, origin, or economic status or that operates in a manner that unreasonably restricts the public's access to the facility.[3] Minutes of a public meeting must be promptly recorded and open to public inspection.[4] Failure to abide by public meeting requirements will invalidate any resolution, rule, or formal action adopted at a meeting.[5] A public officer or member of a governmental entity who violates the Sunshine Law is subject to civil and criminal penalties.[6]

Public Record and Public Meeting Exemptions
The Legislature may provide by general law for the exemption of records and meetings from the requirements of Art. I, s. 24(a) and (b) of the Florida Constitution.[7] The general law must state with specificity the public necessity justifying the exemption[8] and must be no broader than necessary to accomplish its purpose.[9]

Furthermore, the Open Government Sunset Review Act[10] provides that a public record or public meeting exemption may be created or maintained only if it serves an identifiable public purpose. In addition, it may be no broader than necessary to meet one of the following purposes:

[1] Section 286.011(1), F.S.
[2] *Id*.
[3] Section 286.011(6), F.S.
[4] Section 286.011(2), F.S.
[5] Section 286.011(1), F.S.
[6] Section 286.011(3), F.S. Penalties include a fine of up to $500 or a second degree misdemeanor, which is punishable by up to 60 days imprisonment and a $500 fine.
[7] Art. I, s. 24(c), FLA. CONST.
[8] This portion of a public record exemption is commonly referred to as a "public necessity statement."
[9] Art. I, s. 24(c), FLA. CONST.
[10] Section 119.15, F.S.

- Allow the state or its political subdivisions to effectively and efficiently administer a governmental program, which administration would be significantly impaired without the exemption.
- Protect sensitive personal information that, if released, would be defamatory or would jeopardize an individual's safety; however, only the identity of an individual may be exempted under this provision.
- Protect trade or business secrets.[11]

The Open Government Sunset Review Act requires the automatic repeal of a newly created public record or public meeting exemption on October 2nd of the fifth year after creation or substantial amendment, unless the Legislature reenacts the exemption.[12]

Current exemptions for State Agency Cybersecurity Information

Portions of records held by a state agency[13] that contain network schematics, hardware and software configurations, or encryption, or that identify detection, investigation, or response practices for suspected or confirmed cybersecurity[14] incidents,[15] including suspected or confirmed breaches,[16] are confidential and exempt[17] from pubic record requirements if the disclosure of such records would facilitate unauthorized access to or the unauthorized modification, disclosure, or destruction of:

- Data[18] or information, whether physical or virtual; or
- Information technology (IT) resources,[19] which includes:
    - 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

[11] Section 119.15(6)(b), F.S.
[12] Section 119.15(3), F.S.
[13] "State agency" means any official, officer, commission, board, authority, council, committee, or department of the executive branch of state government; the Justice Administrative Commission; and the Public Service Commission. The term includes the Department of Legal Affairs, The Department of Agriculture and Consumer Services, and the Department of Financial Services. The term does not include university boards of trustees or state universities. *See* s. 282.0041(33), F.S.
[14] "Cybersecurity" means the protection afforded to an automated information system in order to attain the applicable objectives of preserving the confidentiality, integrity, and availability of data, information, and information technology resources. *See* s. 282.0041(8), F.S.
[15] "Incident" means a violation or imminent threat of violation, whether such violation is accidental or deliberate, of information technology resources, security, policies, or practices. An imminent threat of violation refers to a situation in which the state agency has a factual basis for believing that a specific incident is about to occur. *See* s. 282.0041(19), F.S.
[16] "Breach" means unauthorized access of data in electronic form containing personal information. Good faith access of personal information by an employee or agent of the covered entity does not constitute a breach of security, provided that the information is not used for a purpose unrelated to the business or subject to further unauthorized use. *See* s. 282.0041(3), F.S.
[17] There is a difference between records the Legislature designates exempt from public record requirements and those the Legislature deems confidential and exempt. A record classified as exempt from public disclosure may be disclosed under certain circumstances. *See WFTV, Inc. v. Sch. Bd. of Seminole*, 874 So.2d 48, 53 (Fla. 5th DCA 2004), review denied 892 So.2d 1015 (Fla. 2004); *City of Rivera Beach v. Barfield*, 642 So.2d 1135 (Fla. 4th DCA 1994); *Williams v. City of Minneola*, 575 So.2d 683, 687 (Fla. 5th DCA 1991). If the Legislature designates a record as confidential and exempt from public disclosure, such record may not be released by the custodian of public records to anyone other than the persons or entities specifically designated in statute. See Op. Att'y Gen. Fla. 04-09 (2004).
[18] "Data" means a subset of structured information in a format that allows such information to be electronically retrieved and transmitted. *See* s. 282.0041(9), F.S.
[19] "Information technology resources" means data processing hardware and software and services, communications, supplies, personnel, facility resources, maintenance, and training. *See* s. 282.0041(22), F.S.

- Security information, whether physical or virtual, which relates to the agency's existing or proposed IT[20] systems.[21,22]

In addition, any portion of a public meeting that would reveal any of the above-described confidential and exempt records is exempt from public meeting requirements. Any portion of an exempt meeting must be recorded and transcribed. The recordings and transcripts are confidential and exempt from public record requirements unless a court of competent jurisdiction, following an in camera review, determines that the meeting was not restricted to the discussion of confidential and exempt data and information. If such a judicial determination occurs, only the portion of the recording or transcript that reveals nonexempt data may be disclosed.[23]

The confidential and exempt cybersecurity information must be available to the Auditor General, the Cybercrime Office within the Florida Department of Law Enforcement (FDLE), the Florida Digital Service (FLDS),[24] and for agencies under the jurisdiction of the Governor, the Chief Inspector General. In addition, the records may be made available to a local government, another state agency, or a federal agency for cybersecurity purposes or in the furtherance of the state agency's official duties.[25]

Current Exemptions for Local Government Cybersecurity Information

Information related to the security of a utility[26] owned or operated by a unit of local government[27] that is designed to protect the utility's networks, computers, programs, and data from attack, damage or unauthorized access, is exempt from public record requirements to the extent disclosure of such information would facilitate the alteration, disclosure, or destruction of data or IT resources.[28]

In addition, information related to the security of existing or proposed IT systems or industrial control technology systems of a utility owned or operated by a unit of local government is exempt from public record requirements to the extent disclosure would facilitate unauthorized access to, and the alternation or destruction of, such IT systems in a manner that would adversely impact the safe and reliable operations of the IT systems and the utility.[29]

Current law also provides a public record exemption for certain cybersecurity information held by supervisor of elections that mirrors the public record exemption for state agencies, which was described above.[30] The confidential and exempt information must be made available to the Auditor General and may be made available to another governmental entity for cybersecurity purposes or in the furtherance of the entity's official duties.[31]

---

[20] "Information technology" means equipment, hardware, software, firmware, programs, systems, networks, infrastructure, media, and related material used to automatically, electronically, and wirelessly collect, receive, access, transmit, display, store, record, retrieve, analyze, evaluate, process, classify, manipulate, manage, assimilate, control, communicate, exchange, convert, converge, interface, switch, or disseminate information of any kind or form. *See* s. 282.0041(20), F.S.

[21] Florida law provides a similar public record exemption for state university and Florida College System institutions. *See* s 1004.055, F.S.

[22] Section 282.318(5), F.S.

[23] Section 282.318(7), F.S. Florida law provides a similar public meeting exemption for state university and Florida College system institutions, *see* s. 1004.055, F.S.

[24] FLDS (formerly the Division of State Technology) is a subdivision of DMS and is charged with overseeing the state's IT resources. Section 20.22(2)(b), F.S.

[25] Section 282.318(8), F.S.

[26] "Utility" means a person or entity that provides electricity, natural gas, telecommunications, water, chilled water, reuse water, or wastewater. Section 119.011(15), F.S.

[27] "Unit of local government" means a county, municipality, special district, local agency, authority, consolidated city-county government, or any other local governmental body or public body corporate or politic authorized or created by general or special law. Section 119.0713(2)(a), F.S.

[28] Section 119.0713 (5)(a)1., F.S.

[29] Section 119.0713(5)(a)2., F.S.

[30] Section 98.015(13)(a), F.S.

[31] Section 98.015(13)(b), F.S.

Critical Infrastructure Cybersecurity

The United States depends on the reliable function of critical infrastructure. Cybersecurity threats exploit the increased complexity and connectivity of critical infrastructure systems, placing the Nation's security, economy, and public safety and health at risk. The World Economic Forum's 2020 Global Risk Report ranked cyberattacks causing disruption to operations and critical infrastructure among the top five increasing global risks.[32]

In 2001, the federal government enacted the Critical Infrastructures Protection Act (act) to protect the increasingly relied upon critical physical and information infrastructures across a vast number of industries.[33] These include telecommunications, energy, financial services, water, and transportation sectors.[34] The act aimed to create a comprehensive and effective program to ensure the continuity of essential functions.[35] "Critical infrastructure" is defined in the act as systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.[36] Recently, the federal government launched an Industrial Control System Cybersecurity Initiative in an attempt to encourage electric utilities and natural gas pipelines to deploy control system cybersecurity technologies to bolster the security and resilience of their facilities.[37] The initiative will be expanded to include the water sector as well.[38]

CS/HB 7055 (2022)

CS/HB 7055, to which this bill is linked, creates cybersecurity related requirements for state agencies and local governments.[39] The bill requires state agencies and local governments to report ransomware incidents and high severity level cybersecurity incidents to the Cybersecurity Operations Center (CSOC) within the FLDS and the Cybercrime Office within FDLE and, in the case of local governments, the sheriff. After the remediation of a cybersecurity incident, the reporting entity must submit an after-action report to FLDS.

The bill requires local governments to adopt cybersecurity standards that safeguard the local government's data, IT, and IT resources by a date certain.

In addition, the bill requires state agency and local government employees to complete certain cybersecurity trainings within 30 days of commencing employment and annually thereafter.

[32] World Economic Forum, *The Global Risks Report 2020*, available at: https://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf (last visited February 19, 2022).
[33] *See* 42 U.S.C. § 5195c.
[34] 42 U.S.C. § 5195c(b)(3).
[35] 42 U.S.C. § 5195c(c)(3).
[36] 42 U.S.C. § 5195c(e).
[37] The White House, *Fact Sheet: Ongoing Public U.S. Efforts to Counter Ransomware* (October 13, 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/13/fact-sheet-ongoing-public-u-s-efforts-to-counter-ransomware/ (last visited February 19, 2022).
[38] *Id*.
[39] CS/HB 7055 (2022) defines "local governments" as counties and municipalities.

Effect of the Bill

The bill provides a general public record exemption in ch. 119, F.S., for the following information held by an agency[40] 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 (OT) systems,[41] or data of an agency.
- Information relating to critical infrastructure.[42]
- Network schematics, hardware and software configurations, or encryption information or information that identifies detection, investigation, or response practices for suspected or confirmed cybersecurity incidents, including suspected or confirmed breaches,[43] if the disclosure of such information would facilitate unauthorized access to or unauthorized modification, disclosure, or destruction of:
    - Data or information, whether physical or virtual; or
    - IT resources, which include an agency's existing or proposed IT systems.
- Cybersecurity incident information reported pursuant to Sections 282.318 or 282.3185, F.S.

The bill also creates a public meeting exemption for any portion of a meeting that would reveal the confidential and exempt information; however, any portion of an exempt meeting must be recorded and transcribed. The recording and transcript are confidential and exempt from public record requirements.

The bill requires the confidential and exempt information to be made available to:

- A law enforcement agency.
- The Auditor General.
- The Cybercrime Office within FDLE.
- The Florida Digital Service.
- For agencies under the jurisdiction of the Governor, the Chief Inspector General.

The bill authorizes the release of the confidential and exempt information:

- In the furtherance of the custodial agency's duties and responsibilities; or
- To another governmental entity in the furtherance of its statutory duties and responsibilities.

The bill also authorizes agencies to report information about cybersecurity incidents in an aggregate format.

The bill provides a public necessity statement as required by the Florida Constitution, and provides for repeal of the exemptions on October 2, 2027, unless reviewed and saved from repeal through reenactment of the Legislature.

The bill repeals duplicative public record and public meetings exemptions for state agencies and supervisors of elections.

---

[40] "Agency" means any state, county, district, authority, or municipal officer, department, division, board, bureau, commission, or other separate unit of government created or established by law including, for the purposes of this chapter, the Commission on Ethics, the Public Service Commission, and the Office of Public Counsel, and any other public or private agency, person, partnership, corporation, or business entity acting on behalf of any public agency.

[41] The bill defines "operational technology" to mean the hardware and software that cause or detect a change through the direct monitoring or control of physical devices, systems, processes, or events.

[42] The bill defines "critical infrastructure" to mean existing and proposed information technology and operational technology systems and assets, whether physical or virtual, the incapacity or destruction of which would negatively affect security, economic security, public health, or public safety.

[43] The bill defines "breach" to mean unauthorized access of data in electronic form containing personal information. Good faith access of personal information by an employee or agent of an agency does not constitute a breach, provided that the information is not used for a purpose unrelated to the business or subject to further unauthorized use.

Effective Date

The bill will become effective on the same date that CS/HB 7055 (2022) takes effect.

II. FISCAL ANALYSIS & ECONOMIC IMPACT STATEMENT

A. FISCAL IMPACT ON STATE GOVERNMENT:

1. Revenues:

None.

2. Expenditures:

See Fiscal Comments.

B. FISCAL IMPACT ON LOCAL GOVERNMENTS:

1. Revenues:

None.

2. Expenditures:

See Fiscal Comments.

C. DIRECT ECONOMIC IMPACT ON PRIVATE SECTOR:

None.

D. FISCAL COMMENTS:

The bill will likely have an insignificant negative fiscal impact on the state and local governments because staff responsible for complying with public record requests may require training related to creation of the public record exemption. In addition, state and local governments could incur costs associated with redacting the confidential and exempt information prior to releasing a record. The costs, however, would be absorbed, as they are part of the day-to-day responsibilities of the agencies.