The Florida Senate

BILL ANALYSIS AND FISCAL IMPACT STATEMENT

(This document is based on the provisions contained in the legislation as of the latest date listed below.)

Prepared By: The Professional Staff of the Committee on Governmental Oversight and Accountability

BILL:	SPB 7020
INTRODUCER:	Governmental Oversight and Accountability Committee
SUBJECT:	OGSR/Agency Cybersecurity Information
DATE:	March 19, 2025
REVISED:	

	ANALYST	STAFF DIRECTOR	REFERENCE	ACTION
1.	Harmsen	McVaney		**GO Submitted as Comm. Bill/Fav**

I. Summary:

SPB 7020 delays for one additional year the repeal of the public record 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's cybersecurity program for the data, information, and state agency IT resources which are held by a state agency, if the disclosure of such portions of records would facilitate 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 also moves up by one year (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 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 meetings laws.

Without action by the Legislature to extend or delete the repeal date, the exemptions in ss. 282.318(5) and (6), F.S., will repeal on October 2, 2025. The bill extends the public records and meeting exemptions for one additional year, setting a new repeal date of October 2, 2026, in order to continue the confidential and exempt status of the information and relevant portions of the meetings. The provisions will be subject to another Open Government Sunset Review in 2026. This will allow the public records and meeting exemptions to be reviewed in concert with the public record and meeting exemptions in s. 119.0725, F.S., which is now also scheduled for an Open Government Sunset Review in 2026.

The bill is not expected to affect state or local government revenues and expenditures.

The bill takes effect October 1, 2025.

II. Present Situation:

Public Records Law

The State Constitution provides that the public has the right to inspect or copy records made or received in connection with official governmental business.[1] This applies to the official business of any public body, officer, or employee of the state, including all three branches of state government, local governmental entities, and any person acting on behalf of the government.[2]

Additional requirements and exemptions that relate to public records are found in various statutes and rules, depending on the branch of government involved.[3] For instance, Legislative records are public pursuant to s. 11.0431, F.S. Public records exemptions for the Legislature are codified primarily in s. 11.0431(2)-(3), F.S., and adopted in the rules of each house of the legislature. Florida Rule of Judicial Administration 2.420 governs public access to judicial branch records.[4] Lastly, ch. 119, F.S., the Public Records Act, provides requirements for public records held by executive agencies and constitutes the main body of public records laws.

The Public Records Act provides that all state, county, and municipal records are open for personal inspection and copying by any person. Each agency has a duty to provide access to public records.[5]

---

[1] FLA. CONST. art. I, s. 24(a).
[2] *Id*. *See also*, *Sarasota Citizens for Responsible Gov't v. City of Sarasota*, 48 So. 3d 755, 762-763 (Fla. 2010).
[3] Chapter 119, F.S., does not apply to legislative or judicial records. *See*, *Locke v. Hawkes*, 595 So. 2d 32, 34 (Fla. 1992); *see also Times Pub. Co. v. Ake*, 660 So. 2d 255 (Fla. 1995).
[4] *State v. Wooten*, 260 So. 3d 1060 (Fla. 4th DCA 2018).
[5] Section 119.01(1), F.S.

Section 119.011(12), F.S., defines "public records" to include:

> [a]ll documents, papers, letters, maps, books, tapes, photographs, films, sound recordings, data processing software, or other material, regardless of the physical form, characteristics, or means of transmission, made or received pursuant to law or ordinance or in connection with the transaction of official business by any agency.

The Florida Supreme Court has interpreted this definition to encompass all materials made or received by an agency in connection with official business which are used to "perpetuate, communicate, or formalize knowledge of some type."[6]

The Florida Statutes specify conditions under which public access to governmental records must be provided. The Public Records Act guarantees every person's right to inspect and copy any state or local government public record at any reasonable time, under reasonable conditions, and under supervision by the custodian of the public record.[7] A violation of the Public Records Act may result in civil or criminal liability.[8]

Only the Legislature may create an exemption to public records requirements.[9] An exemption must be created by general law and must specifically state the public necessity justifying the exemption.[10] Further, the exemption must be no broader than necessary to accomplish the stated purpose of the law. A bill enacting an exemption may not contain other substantive provisions[11] and must pass by a two-thirds vote of the members present and voting in each house of the Legislature.[12]

When creating a public records exemption, the Legislature may provide that a record is "exempt" or "confidential and exempt." There is a difference between records the Legislature has determined to be exempt from the Public Records Act and those which the Legislature has determined to be exempt from the Public Records Act *and confidential*.[13] Records designated as "confidential and exempt" are not subject to inspection by the public and may only be released under the circumstances defined by statute.[14] Records designated as "exempt" may be released at the discretion of the records custodian under certain circumstances.[15]

---

[6] *Shevin v. Byron, Harless, Schaffer, Reid and Assoc. Inc*., 379 So. 2d 633, 640 (Fla. 1980).
[7] Section 119.07(1)(a), F.S.
[8] Section 119.10, F.S. Public records laws are found throughout the Florida Statutes, as are the penalties for violating those laws.
[9] FLA. CONST. art. I, s. 24(c).
[10] *Id*.
[11] The bill may, however, contain multiple exemptions that relate to one subject.
[12] FLA. CONST. art. I, s. 24(c)
[13] *WFTV, Inc. v. The Sch. Bd. of Seminole County*, 874 So. 2d 48, 53 (Fla. 5th DCA 2004).
[14] *Id*.
[15] *Williams v. City of Minneola*, 575 So. 2d 683 (Fla. 5th DCA 1991).

General exemptions from the public records requirements are typically contained in the Public Records Act.[16] Specific exemptions are often placed in the substantive statutes which relate to a particular agency or program.[17]

Open Meetings Laws

The State Constitution provides that the public has a right to access governmental meetings.[18] Each collegial body must provide notice of its meetings to the public and permit the public to attend any meeting at which official acts are taken or at which public business is transacted or discussed.[19] This applies to the meetings of any collegial body of the executive branch of state government, counties, municipalities, school districts, or special districts.[20]

Public policy regarding access to government meetings also is addressed in the Florida Statutes. Section 286.011, F.S., which is also known as the "Government in the Sunshine Law"[21] or the "Sunshine Law,"[22] requires all meetings of any board or commission of any state or local agency or authority at which official acts are taken be open to the public.[23] The board or commission must provide the public reasonable notice of such meetings.[24] 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 which operates in a manner that unreasonably restricts the public's access to the facility.[25] Minutes of a public meeting must be promptly recorded and open to public inspection.[26] Failure to abide by open meetings requirements will invalidate any resolution, rule, or formal action adopted at a meeting.[27] A public officer or member of a governmental entity who violates the Sunshine Law is subject to civil and criminal penalties.[28]

The Legislature may create an exemption to open meetings requirements by passing a general law by a two-thirds vote of the House and the Senate.[29] The exemption must explicitly lay out the public necessity justifying the exemption and be no broader than necessary to accomplish the

[16] *See, e.g.*, s.119.071(1)(a), F.S., exempting from public disclosure examination questions and answer sheets of exams administered by a governmental agency for the purpose of licensure.
[17] *See, e.g.*, s. 213.053(2), F.S., exempting from public disclosure information received by the DOR, including investigative reports and information.
[18] FLA. CONST., art. I, s. 24(b).
[19] *Id*.
[20] FLA. CONST., art. I, s. 24(b). Meetings of the Legislature are governed by Article III, section 4(e) of the Florida Constitution, which states: "The rules of procedure of each house shall further provide that all prearranged gatherings, between more than two members of the legislature, or between the governor, the president of the senate, or the speaker of the house of representatives, the purpose of which is to agree upon formal legislative action that will be taken at a subsequent time, or at which formal legislative action is taken, regarding pending legislation or amendments, shall be reasonably open to the public."
[21] *Times Pub. Co. v. Williams*, 222 So.2d 470, 472 (Fla. 2d DCA 1969).
[22] *Board of Public Instruction of Broward County v. Doran*, 224 So.2d 693, 695 (Fla. 1969).
[23] Section 286.011(1)-(2), F.S.
[24] *Id*.
[25] Section 286.011(6), F.S.
[26] Section 286.011(2), F.S.
[27] Section 286.011(1), F.S.
[28] Section 286.011(3), F.S.
[29] FLA. CONST., art. I, s. 24(c).

stated purpose of the exemption.[30] A statutory exemption which does not meet these two criteria may be unconstitutional and may not be judicially saved.[31]

State Cybersecurity Act

The State Cybersecurity Act[32] (the Cybersecurity Act) requires the Department of Management Services (DMS), acting through the Florida Digital Services (FLDS), to establish standards and processes for assessing state agencies' cybersecurity risks and determine appropriate security measures. Additionally, the DMS must:[33]

- Adopt rules to mitigate risk and to safeguard state agency digital assets, data, information, and IT resources to ensure its confidentiality and integrity;
- Develop an annual cybersecurity strategic plan which includes the identification and mitigation of risk, proactive protections against threats, and threat reporting and response and recovery protocols for a cyber incident;
- Publish an IT security framework for use by state agencies;
- Annually review state agencies' strategic and operational cybersecurity plans; and
- Operate a Cybersecurity Operations Center (CSOC), which serves as "a clearinghouse for threat information" and coordinates with the Department of Law Enforcement to support state agencies with their response to a confirmed or suspected cybersecurity incident.

Each agency is also vested with responsibilities under the Cybersecurity Act, which include:[34]

- Creating a cybersecurity response team which convenes upon notice of a cybersecurity incident and reports on all confirmed or suspected incidents;
- Submitting an annual report on the agency's strategic and operational cybersecurity plans;
- Performing a triennial comprehensive risk assessment to determine security threats to the agency
- Developing internal procedures, including for reporting cybersecurity incidents and breaches to the Cybercrime Office and the FLDS;
- Receiving recommendations from the DMS regarding identified risks to agency data, information, and IT resources, and implementation of safeguards and risk assessment remediation plans to resolve the risk;
- Ensuring the performance of periodic internal audits and evaluations of the agency's cybersecurity program for the data, information, and IT resources of the agency; and
- Submitting an after-action report, including a summary of "insights gained as a result of the incident" to the FLDS within 1 week after the agency's resolution or remediation of a cybersecurity incident or ransomware incident.

[30] *Id*.
[31] *See supra* note 10.
[32] Section 282.318(1), F.S.
[33] Section 282.318(3), F.S.
[34] Section 282.318(4), F.S.

Public Records Exemptions for Cybersecurity Information

The Cybersecurity Act ultimately requires the creation of documents and communications that are likely to contain highly sensitive information, that may reveal vulnerabilities in state agency data or cybersecurity.

For example, the Office of the Inspector General conducts state agency cybersecurity audits pursuant to s. 20.055(6)(i), F.S, and each state agency Inspector General is required to incorporate a specific cybersecurity audit plan into their annual audit planning process.[35] Additionally, the Auditor General "regularly conduct information technology audits of governmental entities pursuant to s. 11.45, F.S."[36] Further, agencies are required to communicate incident reports and after-action reports regarding hacking events to specific governmental entities.

Section 282.318(4), F.S., Exemptions

The Cybersecurity Act provides that the following state agency information is confidential and exempt from public record requirements:

- Comprehensive risk assessments, whether completed by the agency itself or a private vendor;[37]
- Internal policies and procedures that, if disclosed, could facilitate the unauthorized modification, disclosure, or destruction of data or IT resources;[38] and
- The results of internal cybersecurity audits and evaluations.[39]

This information must be made available to the Auditor General, the Cybercrime Office of the Florida Department of Law Enforcement, the FLDS, and—for agencies under the jurisdiction of the Governor—the Chief Inspector General.

Section 282.318(5), F.S., Exemptions

In 2016, the Legislature created s. 282.318(5), F.S., which more generally designates as confidential and exempt from public record requirements the portions of risk assessments,[40] evaluations, external audits,[41] and other reports of a state agency's cybersecurity program for the data, information, and state agency IT resources[42] held by a state agency if the disclosure of such

[35] Florida Office of Inspector General, *Cybersecurity Resources*, https://www.floridaoig.com/cyberSecurity.htm (last visited Jan. 20, 2025). *See, e.g.*, Florida Department of Health Office of Inspector General, Internal Audit Report # 2223-001 (June 5, 2024), https://www.floridahealth.gov/about/administrative-functions/inspector-general/A-2324-001FinalReport.pdf (last visited Jan. 20, 2025).
[36] Florida Office of the Auditor General, Open Government Sunset Review Questionnaire (Cybersecurity Risk Assessments and Audits) (September 2024) (on file with the Senate Governmental Oversight and Accountability Committee).
[37] Section 282.318(4)(d), F.S.
[38] Section 282.318(4)(e), F.S.
[39] Section 282.318(4)(g), F.S.
[40] Section 282.0041(29) defines a "risk assessment" for purposes of ch. 282, F.S., as the "process of identifying security risks, determining their magnitude, and identifying areas needing safeguards."
[41] For purposes of subsection (5) of s. 282.318, F.S., an "external audit" is defined as one conducted by an entity other than the state agency that is the subject of the audit.
[42] Section 282.0041(22), F.S., defines "IT resources" as data processing hardware and software services, communications, supplies, personnel, facility resources, maintenance, and training.

portions of records would facilitate 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.

An agency *must* disclose this information only to the Auditor General, the Cybercrime Office of the FDLE, the FLDS, and—for agencies under the Governor's jurisdiction—the Chief Inspector General. Portions of records *may* be made available to a local government, another state agency, or a federal agency for cybersecurity purposes or in furtherance of the state agency's official duties.[43]

The 2016 public necessity statement for this public record exemption, found that independent, external review of state agency cybersecurity information and related systems was valuable.[44] The bill's public necessity statement further provided as a basis for the public record exemption that:

> Such documents would likely include an analysis of the state agency's current [IT] program or systems which could clearly identify vulnerabilities or gaps in current systems or processes and propose recommendations to remedy identified vulnerabilities. The disclosure of such portions of records would jeopardize the [IT] security of the state agency, and compromise the integrity and availability of agency data and [IT] resources, which would significantly impair the administration of governmental programs.

Section 119.0725, F.S., Exemptions

Florida law also has a similar public record exemption in s. 119.0725, F.S., which makes confidential and exempt from public record requirements:[45]

- Coverage limits and deductible or self-insurance amounts of insurance or other risk mitigation coverages acquired for the protection of IT systems, operational technology[46] systems, or an agency's data;
- Information relating to "critical infrastructure", defined as existing and proposed IT and operational technology systems and assets (physical or virtual), the incapacity or destruction of which would negatively affect security, economic security, public health, or public safety;

[43] Section 282.382(7), F.S.
[44] Chapter 2016-114, Laws of Fla. *See also*, Senate Bill 624 (2016).
[45] Section 119.0725(2), F.S. This public record exemption was implemented in 2022, after s. 282.318, F.S., was passed, to better address ransomware incidents.
[46] "Operational technology" is the hardware and software that causes or detects a change through the direct monitoring or control of physical devices, systems, processes, or events. Section 119.0725(1)(g), F.S.

- Cybersecurity incident information reported by state agencies or local governments pursuant to ss. 282.318 and 282.3185, F.S.; and
- Network schematics; hardware and software configurations; encryption information; or information that identifies detection, investigation, or response practices for suspected or confirmed cybersecurity incidents, including suspected or confirmed breaches, if the disclosure of such information would facilitate unauthorized access to or unauthorized modification, disclosure, or destruction of:
  - Data[47] or information (physical or virtual); or
  - IT resources, which include an agency's existing or proposed IT systems.

An agency *must* make this information available to a law enforcement agency, the Auditor General, the Cybercrime Office of the FDLE, the FLDS, and—for agencies under the jurisdiction of the Governor—the Chief Inspector General. An agency *may* disclose the information confidential and exempt information addressed in s. 119.0725, F.S., "in the furtherance of its official duties and responsibilities or to another agency or governmental entity in the furtherance of its statutory duties and responsibilities."[48]

Agencies must still report information about cybersecurity incidents in the aggregate.[49]

Portions of this exemption were previously included in s. 282.318, F.S., until 2022, when the general exemption for specific cybersecurity information in s. 119.075, F.S., was created.[50]

Section 119.0725(3), F.S., also creates a public meeting exemption for any portion of a meeting that would reveal the information made confidential and exempt pursuant to s. 119.0725(2), F.S.; however, any portion of an exempt meeting must be recorded and transcribed. The recording and transcript are confidential and exempt from public record inspection and copying requirements.

These exemptions are currently scheduled to undergo an Open Government Sunset Review and repeal on October 2, 2027.

Cybersecurity Advisory Council

The Florida Cybersecurity Task Force (Task Force) was created in 2019[51] to "review and conduct an assessment of the state's cybersecurity infrastructure, governance, and operations." The Task Force produced a final report of its findings and recommendations on February 1, 2021, after which, the body expired.

In 2021, the Legislature subsequently created the Florida Cybersecurity Advisory Council (Advisory Council) within the DMS.[52] The Advisory Council's duties, generally, are to meet on a quarterly basis to review Florida's current cybersecurity policy and recommend changes. The

[47] "Data" is the subset of structured information in a format that allows such information to be electronically retrieved and transmitted. Section 282.0041(9), F.S.
[48] Section 119.0725(5), F.S.
[49] Section 119.0725(6), F.S.
[50] See ch. 2022-220, Laws of Fla.
[51] Chapter 2019-118, s. 29, Laws of Fla.
[52] Chapter 2021-234, s. 7, Laws of Fla.

Advisory Council is specifically tasked with assessing ongoing risks to state agency IT and critical cyber infrastructure; recommending a reporting and information sharing system to notify state agencies of new risks; recommending data breach simulation exercises; assisting with the development of cybersecurity best practice recommendations; assessing cybersecurity and ransomware incident reporting from state agencies, counties, and municipalities; and examining inconsistencies between state and federal law regarding cybersecurity.[53]

The Advisory Council must also annually submit two separate reports: the first to the President of the Senate and Speaker of the House of Representatives which details legislative recommendations the Advisory Council considers necessary; the second to the Governor, President of the Senate, and Speaker of the House of Representatives, which reports the data, trends, analysis, and recommendations for state and local action regarding ransomware incidents.

The membership of the Advisory Council consists of up to 19 members, including the Lieutenant Governor, state chief information officer, state chief information security officer, and various other members from state agencies and the public. The members are required to maintain the confidential or exempt status of information they receive in the performance of their duties and responsibilities as members of the council.[54]

Of the 52 meetings held by the Advisory Council's workgroups between June 28, 2022, and November 7, 2024, one had a general meeting portion open to the public—the rest of the "executive sessions" were shaded meetings and generally did not offer a specific citation as the basis for the meeting's closure.[55]

Open Government Sunset Review Act

The provisions of s. 119.15, F.S., known as the Open Government Sunset Review Act (the Act), prescribe a legislative review process for newly created or substantially amended public records or open meetings exemptions,[56] with specified exceptions.[57] The Act requires the repeal of such exemption on October 2nd of the fifth year after creation or substantial amendment. In order to save an exemption from repeal, the Legislature must reenact the exemption or repeal the sunset date.[58] In practice, many exemptions are continued by repealing the sunset date, rather than reenacting the exemption.

The Act provides that a public records or open meetings exemption may be created or maintained only if it serves an identifiable public purpose and is no broader than is necessary.[59] An exemption serves an identifiable purpose if the Legislature finds that the purpose of the

[53] Section 282.319, F.S.
[54] Section 282.319(8), F.S.
[55] Florida Department of Management Services, Cybersecurity Advisory Council, *Advisory Council Overview: Workgroups*, https://www.dms.myflorida.com/other_programs/cybersecurity_advisory_council (last visited Jan. 8, 2025).
[56] Section 119.15, F.S. Section 119.15(4)(b), F.S., provides that an exemption is considered to be substantially amended if it is expanded to include more records or information or to include meetings.
[57] Section 119.15(2)(a) and (b), F.S., provides that exemptions required by federal law or applicable solely to the Legislature or the State Court System are not subject to the Open Government Sunset Review Act.
[58] Section 119.15(3), F.S.
[59] Section 119.15(6)(b), F.S.

exemption outweighs open government policy and cannot be accomplished without the exemption and it meets one of the following purposes:

- It allows the state or its political subdivision to effectively and efficiently administer a program and administration would be significantly impaired without the exemption;[60]
- It protects sensitive, personal information, the release of which would be defamatory or would jeopardize an individual's safety. If this public purpose is cited as the basis of an exemption, however, only personal identifying information is exempt;[61] or
- It protects trade or business secrets.[62]

The Act also requires specified questions to be considered during the review process.[63] In examining an exemption, the Act directs the Legislature to question the purpose and necessity of reenacting the exemption.

If the exemption is continued and expanded, then a public necessity statement and a two-thirds vote for passage are again required.[64] If the exemption is reenacted or saved from repeal without substantive changes or if the exemption is narrowed, then a public necessity statement and a two-thirds vote for passage are *not* required. If the Legislature allows an exemption to expire, the previously exempt records will remain exempt unless otherwise provided by law.[65]

Open Government Sunset Review of the Public Records and Open Meetings Exemptions for Cybersecurity Information

The staff of the Senate Governmental Oversight and Accountability Committee and the House Government Operations Subcommittee jointly surveyed Florida agencies to ascertain whether the public record and open meeting exemptions in s. 282.318(5) and (6), F.S., remain necessary. Staff reviewed a total of 24 agencies' responses, a majority of which recommend that the Legislature reenact the public record exemptions without any changes.

Public Record Exemption Findings

Legislative staff requested that respondents consider the public records exemption for cybersecurity in s. 119.0725, F.S., to determine if there is any overlap between those provisions and the exemption under review. Some respondents noted that s. 119.0725, F.S., did have some overlap with s. 119.0713(5), F.S.; however, many of those that gave such feedback noted that s. 119.0725, F.S., did not include the full breadth of the information protected by s. 282.318, F.S.

[60] Section 119.15(6)(b)1., F.S.
[61] Section 119.15(6)(b)2., F.S.
[62] Section 119.15(6)(b)3., F.S.
[63] Section 119.15(6)(a), F.S. The specified questions are:
- What specific records or meetings are affected by the exemption?
- Whom does the exemption uniquely affect, as opposed to the general public?
- What is the identifiable public purpose or goal of the exemption?
- Can the information contained in the records or discussed in the meeting be readily obtained by alternative means? If so, how?
- Is the record or meeting protected by another exemption?
- Are there multiple exemptions for the same type of record or meeting that it would be appropriate to merge?

[64] FLA. CONST. art. I, s. 24(c).
[65] Section 119.15(7), F.S.

Further, many respondents noted that, unless several provisions of s. 282.318(5), F.S., were imported verbatim into s. 119.0725, F.S., there would be a loss in information currently protected if the chapter 282, F.S., provision was not reenacted.

The responding agencies generally did not report any issue interpreting or applying the exemptions, and noted that the exemptions were used, in particular, to protect relevant portions of audits, security incident reports, and security protocols.

Responding agencies also state that they share the confidential and exempt documents with the Office of Inspect General, Auditor General, FLDS, and FDLE, usually for audit or reporting purposes. At least one agency cites sharing exempt information with the Executive Office of the Governor, IRS, FBI, Social Security Administration, Centers for Medicare and Medicaid Services, U.S. Department of Health and Human Services, Multi-State Information Sharing and Analysis Center (MS-ISAC), and federal Cybersecurity & Infrastructure Security Agency, for either incident reporting, required auditing, or in order to meet a federal funding requirement.

The Legislature is directed to consider whether the records subject to an Open Government Sunset Review are protected by another exemption, and if so, if it would be appropriate to merge the exemptions.[66] As outlined above, there are at least three public record exemptions that may cover information made confidential and exempt by s. 282.318(5), F.S. Several agencies seem to rely on the exemptions as a group to protect "cybersecurity information" rather than distinguish between them.

Public Meeting Exemption Findings

Few responding agencies report using the public meeting exemption in s. 282.318(6), F.S., which exempts those portions of a public meeting that would reveal records which are confidential and exempt under s. 282.318(5), F.S. Of the nine respondents who provided feedback regarding the public meeting exemption in s. 282.318(6), F.S., all but one supported its reenactment without any change.

One respondent reports using the exemption in IT procurement meetings that include cybersecurity discussions. The DMS reports using the exemption approximately 20 times for incident response meetings, risk assessment meetings, audit meetings, and assessment meetings—it is unclear whether this number includes the Cybersecurity Advisory Council's meetings throughout the year.

III. Effect of Proposed Changes:

The bill delays for one year the repeal of the public records exemption and related public meeting exemption for portions of risk assessments, evaluations, external audits, and other reports of a state agency's cybersecurity program for the data, information, and state agency IT resources which are held by a state agency, if the disclosure of such portions of records would facilitate unauthorized access to, or the unauthorized modification, disclosure, or destruction of:

- Data or information, whether physical or virtual; or
- IT resources, which include:

[66] Section 119.15(6)(a), F.S.

- 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, that relates to the agency's existing or proposed IT systems.

These exemptions will repeal on October 2, 2025, if this bill does not become law.

The bill extends the repeal date for the public records exemption for specific cybersecurity information in s. 282.318(5) and the related public meeting exemption in s. 282.318(6) for an additional 2 years, from October 2, 2025, until October 2, 2026.

Conversely, the bill moves up by one year (to October 2, 2026), the Open Government Sunset Review for the public record and public meeting exemptions in s. 119.0725(2) and (3), F.S. This 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 meetings laws.

This will allow the two exemptions to be assessed at the same time.

IV. Constitutional Issues:

A. Municipality/County Mandates Restrictions:

Not applicable. The bill does not require counties or municipalities to take an action requiring the expenditure of funds, reduce the authority that counties or municipalities have to raise revenue in the aggregate, nor reduce the percentage of state tax shared with counties or municipalities.

B. Public Records/Open Meetings Issues:

Vote Requirement

Article I, s. 24(c) of the State Constitution requires a two-thirds vote of the members present and voting for final passage of a bill creating or expanding an exemption to the public records disclosure requirements or public meeting requirements. This bill

continues a current public records exemption and a public meeting exemption beyond the current date of repeal and moves up another public record and public meeting exemption; thus, the bill does not require an extraordinary vote for enactment.

Public Necessity Statement

Article I, s. 24(c) of the State Constitution requires a bill creating or expanding an exemption to the public records disclosure requirements to state with specificity the public necessity justifying the exemption. This bill continues a current public records exemption without creating a new exemption or expanding the current exemption, and therefore does not require a public necessity statement.

Breadth of Exemption

This bill does not expand or narrow the breadth of the exemption provided for in prior law. Article I, s. 24(c) of the State Constitution requires an exemption to the public records requirements to be no broader than necessary to accomplish the stated purpose of the law. The purpose of the law is to protect information relating to state agency cybersecurity which could make the state more vulnerable to attack or other criminal activity. This bill exempts only those portions of records and meetings that contain relevant information and therefore does not appear to be broader than necessary to accomplish the purposes of the law.

C. Trust Funds Restrictions:

None identified.

D. State Tax or Fee Increases:

None identified.

E. Other Constitutional Issues:

None identified.

V. Fiscal Impact Statement:

A. Tax/Fee Issues:

None identified.

B. Private Sector Impact:

The private sector will continue to be subject to the cost associated with an agency's review and redaction of exempt records in response to a public record request for information covered by s. 282.318(5), F.S.

C. Government Sector Impact:

The government sector will continue to incur costs related to the review and redaction of exempt records associated with responding to public records requests.

VI. Technical Deficiencies:

None.

VII. Related Issues:

None.

VIII. Statutes Affected:

This bill substantially amends sections 282.318 and 119.0725 of the Florida Statutes.

IX. Additional Information:

A. Committee Substitute – Statement of Changes:
(Summarizing differences between the Committee Substitute and the prior version of the bill.)

None.

B. Amendments:

None.