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 Innovation, Industry, and Technology

BILL:	SB 1170
INTRODUCER:	Senator Baxley
SUBJECT:	Public Records and Meetings/Division of State Technology
DATE:	January 10, 2020 REVISED:

	ANALYST	STAFF DIRECTOR	REFERENCE	ACTION
1.	Wiehle	Imhof	IT	**Pre-meeting**
2.			GO	
3.			RC	

I. Summary:

SB 1170 amends two existing public records exemptions. While the bill makes numerous changes, the net effect is to: add "network schematics, hardware and software configurations, and encryption" records to an existing exemption; streamline and simplify the exemptions by deleting duplicative provisions and restructuring the remaining provisions to maintain the same effect; and provide for Open Government Sunset Review and automatic repeal of both amended exemptions.

The bill also creates a public meetings exemption for those portions of a public meeting which would reveal records that the above-discussed provisions makes exempt. No exempt portion of an exempt meeting may be off the record, but must be recorded and transcribed. A recording and transcript is confidential and exempt from disclosure unless a court of competent jurisdiction, after an in camera review, determines that the meeting was not restricted to the discussion of data and information made confidential and exempt by this section. In the event of such a judicial determination, only that portion of the recording and transcript which reveals nonexempt data and information may be disclosed to a third party.

II. Present Situation:

Access to Public Records - Generally

The Florida Constitution provides that the public has the right to inspect or copy records made or received in connection with official governmental business.[1] The right to inspect or copy 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]

[1] FLA. CONST. art. I, s. 24(a).
[2] *Id*.

Additional requirements and exemptions related to public records are found in various statutes and rules, depending on the branch of government involved. For instance, section 11.0431, Florida Statutes (F.S.), provides public access requirements for legislative records. Relevant exemptions are codified in s. 11.0431(2)-(3), F.S., and the statutory provisions are adopted in the rules of each house of the legislature.[3] Florida Rule of Judicial Administration 2.420 governs public access to judicial branch records.[4] Lastly, chapter 119, F.S., provides requirements for public records held by executive agencies.

Executive Agency Records – The Public Records Act

Chapter 119, F.S., known as the Public Records Act, provides that all state, county, and municipal records are open for personal inspection and copying by any person, and that providing access to public records is a duty of each agency.[5]

A public record includes virtually any document or recording, regardless of its physical form or how it may be transmitted.[6] The Florida Supreme Court has interpreted the statutory definition of "public record" to include "material prepared in connection with official agency business which is intended to perpetuate, communicate, or formalize knowledge of some type.[7]

The Florida Statutes specify conditions under which public access to public records must be provided. The Public Records Act guarantees every person's right to inspect and copy any public record at any reasonable time, under reasonable conditions, and under supervision by the custodian of the public record.[8] A violation of the Public Records Act may result in civil or criminal liability.[9]

The Legislature may exempt public records from public access requirements by passing a general law by a two-thirds vote of both the House and the Senate.[10] The exemption must state with specificity the public necessity justifying the exemption and must be no broader than necessary to accomplish the stated purpose of the exemption.[11]

---

[3] *See* Rule 1.48, *Rules and Manual of the Florida Senate*, (2018-2020) and Rule 14.1, *Rules of the Florida House of Representatives*, Edition 2, (2018-2020)

[4] *State v. Wooten*, 260 So. 3d 1060 (Fla. 4th DCA 2018).

[5] Section 119.01(1), F.S. Section 119.011(2), F.S., defines "agency" as "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."

[6] Section 119.011(12), F.S., defines "public record" to mean "all 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."

[7] *Shevin v. Byron, Harless, Schaffer, Reid and Assoc., Inc*., 379 So. 2d 633, 640 (Fla. 1980).

[8] Section 119.07(1)(a), F.S.

[9] Section 119.10, F.S. Public records laws are found throughout the Florida Statutes, as are the penalties for violating those laws.

[10] FLA. CONST. art. I, s. 24(c).

[11] *Id*. *See, e.g., Halifax Hosp. Medical Center v. News-Journal Corp.*, 724 So. 2d 567 (Fla. 1999) (holding that a public meetings exemption was unconstitutional because the statement of public necessity did not define important terms and did

General exemptions from the public records requirements are contained in the Public Records Act.[12] Specific exemptions often are placed in the substantive statutes relating to a particular agency or program.[13]

When creating a public records exemption, the Legislature may provide that a record is "exempt" or "confidential and exempt." Custodians of records designated as "exempt" are not prohibited from disclosing the record; rather, the exemption means that the custodian cannot be compelled to disclose the record.[14] Custodians of records designated as "confidential and exempt" may not disclose the record except under circumstances specifically defined by the Legislature.[15]

Open Meetings Law

The Florida Constitution provides that the public has a right to access governmental meetings.[16] 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.[17] This applies to the meetings of any collegial body of the executive branch of state government, counties, municipalities, school districts or special districts.[18]

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,"[19] or the "Sunshine Law,"[20] requires all meetings of any board or commission of any state or local agency or authority at which official acts are to be taken be open to the public.[21] The board or commission must provide the public reasonable notice of such meetings.[22] 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.[23] Minutes of a public meeting must be promptly recorded and open to public

---

not justify the breadth of the exemption); *Baker County Press, Inc. v. Baker County Medical Services, Inc.*, 870 So. 2d 189 (Fla. 1st DCA 2004) (holding that a statutory provision written to bring another party within an existing public records exemption is unconstitutional without a public necessity statement).

[12] *See, e.g.*, s. 119.071(1)(a), F.S. (exempting from public disclosure examination questions and answer sheets of examinations administered by a governmental agency for the purpose of licensure).

[13] *See, e.g.*, s. 213.053(2)(a), F.S. (exempting from public disclosure information contained in tax returns received by the Department of Revenue).

[14] *See Williams v. City of Minneola*, 575 So. 2d 683, 687 (Fla. 5th DCA 1991).

[15] *WFTV, Inc. v. The School Board of Seminole*, 874 So. 2d 48 (Fla. 5th DCA 2004).

[16] FLA CONST.., art. I, s. 24(b).

[17] *Id*.

[18] 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."

[19] *Times Pub. Co. v. Williams*, 222 So. 2d 470, 472 (Fla. 2d DCA 1969).

[20] *Board of Public Instruction of Broward County v. Doran*, 224 So. 2d 693, 695 (Fla. 1969).

[21] Section 286.011(1)-(2), F.S.

[22] *Id*.

[23] Section 286.011(6), F.S.

inspection.[24] Failure to abide by public meetings requirements will invalidate any resolution, rule or formal action adopted at a meeting.[25] A public officer or member of a governmental entity who violates the Sunshine Law is subject to civil and criminal penalties.[26]

The Legislature may create an exemption to public meetings requirements by passing a general law by at least a two-thirds vote of both the Senate and the House of Representatives.[27] The exemption must explicitly lay out the public necessity justifying the exemption, and must be no broader than necessary to accomplish the stated purpose of the exemption.[28] A statutory exemption which does not meet these two criteria may be unconstitutional and may not be judicially saved.[29]

The following are general exemptions from the requirement that all meetings of any state agency or authority be open to the public:

- That portion of a meeting that would reveal a security or fire safety system plan; and
- Any portion of a team meeting at which negotiation strategies are discussed.[30]

Open Government Sunset Review Act

The Open Government Sunset Review Act[31] (the act) prescribes a legislative review process for newly created or substantially amended[32] public records or open meetings exemptions, with specified exceptions.[33] It requires the automatic repeal of such exemption on October 2nd of the fifth year after creation or substantial amendment, unless the Legislature reenacts the exemption.[34]

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.[35] An exemption serves an identifiable purpose if it meets one of the following purposes *and* the Legislature finds that the purpose of the exemption outweighs open government policy and cannot be accomplished without the exemption:

---

[24] Section 286.011(2), F.S.
[25] Section 286.011(1), F.S.
[26] Section 286.011(3), F.S.
[27] FLA CONST., art. I, s. 24(c).
[28] *Id*.
[29] *Halifax Hosp. Medical Center v. New-Journal Corp.,* 724 So. 2d 567 (Fla. 1999). In *Halifax Hospital*, the Florida Supreme Court found that a public meetings exemption was unconstitutional because the statement of public necessity did not define important terms and did not justify the breadth of the exemption. *Id*. at 570. The Florida Supreme Court also declined to narrow the exemption in order to save it. *Id.* In *Baker County Press, Inc. v. Baker County Medical Services, Inc.*, 870 So. 2d 189 (Fla. 1st DCA 2004), the court found that the intent of a public records statute was to create a public records exemption. The *Baker County Press* court found that since the law did not contain a public necessity statement, it was unconstitutional. *Id*. at 196.
[30] Section 286.0113, F.S.
[31] Section 119.15, F.S.
[32] An exemption is considered to be substantially amended if it is expanded to include more records or information or to include meetings as well as records. Section 119.15(4)(b), F.S.
[33] Section 119.15(2)(a) and (b), F.S., provide that exemptions that are required by federal law or are applicable solely to the Legislature or the State Court System are not subject to the Open Government Sunset Review Act.
[34] Section 119.15(3), F.S.
[35] Section 119.15(6)(b), F.S.

- It allows the state or its political subdivisions to effectively and efficiently administer a governmental program, and administration would be significantly impaired without the exemption;[36]
- It protects sensitive, personal information, the release of which would be defamatory, cause unwarranted damage to the good name or reputation of the individual, or would jeopardize the individual's safety. If this public purpose is cited as the basis of an exemption, however, only personal identifying information is exempt;[37] or
- It protects information of a confidential nature concerning entities, such as trade or business secrets.[38]

The act also requires specified questions to be considered during the review process.[39] In examining an exemption, the act directs the Legislature to carefully 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 required.[40] If the exemption is continued without substantive changes or if the exemption is continued and narrowed, then a public necessity statement and a two-thirds vote for passage are *not* required. If the Legislature allows an exemption to sunset, the previously exempt records will remain exempt unless provided for by law.[41]

Security of State Agency Data and Information Technology

Section 282.318, F.S., is the Information Technology Security Act. It makes the Department of Management Services (department) responsible for the security of data and information technology for all state agencies.[42] The department's responsibilities include:

- Developing and annually updating a statewide information technology security strategic plan that includes security goals and objectives, risk management, incident management, and disaster recovery planning;
- Establishing asset management procedures;
- Completing comprehensive risk assessments;

[36] Section 119.15(6)(b)1., F.S.
[37] Section 119.15(6)(b)2., F.S.
[38] Section 119.15(6)(b)3., F.S.
[39] 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?

[40] *See generally* s. 119.15, F.S.
[41] Section 119.15(7), F.S.
[42] For these purposes, the term state agencies includes any official, officer, commission, board, authority, council, committee, or department of the executive branch of state government, including the Department of Legal Affairs, the Department of Agriculture and Consumer Services, and the Department of Financial Services; the Justice Administrative Commission; and the Public Service Commission,. The term does not include university boards of trustees or state universities. ss. 282.319(2) and 282.0041(27), F.S.

- Identifying protection procedures;
- Establishing agency computer security incident response teams for responding to security incidents;
- Developing agency strategic and operational information technology security plans; and
- Establishing the safeguards for protecting data and information technology resources.

Each state agency is required to conduct, and update every three years, a risk assessment to determine the security threats to data, information, and information technology resources. The risk assessment is confidential and exempt from s. 119.07(1), F.S, except that it is available to the Auditor General, the Division of State Technology within the department, the Cybercrime Office of the Department of Law Enforcement, and, for state agencies under the jurisdiction of the Governor, the Chief Inspector General.[43]

Each state agency is required to develop, and periodically update, written internal policies and procedures, which include procedures for reporting information technology security incidents and breaches to the Cybercrime Office of the Department of Law Enforcement and the Division of State Technology within the department, and which must be consistent with the rules, guidelines, and processes established by the department to ensure the security of the data, information, and information technology resources of the agency. The internal policies and procedures that, if disclosed, could facilitate the unauthorized modification, disclosure, or destruction of data or information technology resources are confidential information and exempt from s. 119.07(1), F.S., except that the information is available to the Auditor General, the Cybercrime Office of the Department of Law Enforcement, the Division of State Technology within the department, and, for state agencies under the jurisdiction of the Governor, the Chief Inspector General.[44]

Each state agency is required to conduct periodic internal audits and evaluations of the agency's information technology security program for the data, information, and information technology resources of the agency. The results of these audits and evaluations are confidential information and exempt from s. 119.07(1), F.S., except that such information is available to the Auditor General, the Cybercrime Office of the Department of Law Enforcement, the Division of State Technology within the department, and, for agencies under the jurisdiction of the Governor, the Chief Inspector General.[45]

Each state agency is required to develop a process for detecting, reporting, and responding to threats, breaches, or information technology security incidents which is consistent with the security rules, guidelines, and processes established by the Agency for State Technology. All information technology security incidents and breaches must be reported to the Division of State Technology within the department and the Cybercrime Office of the Department of Law Enforcement. Records held by a state agency which identify detection, investigation, or response practices for suspected or confirmed information technology security incidents, including suspected or confirmed breaches, are confidential and exempt from s. 119.07(1), F.S, and

[43] Section 282.318(4)(d), F.S.
[44] Section 282.318(4)(e), F.S.
[45] Section 282.318(4)(g), F.S.

s. 24(a), Art. I of the State Constitution, if the disclosure of such records would facilitate unauthorized access to or the unauthorized modification, disclosure, or destruction of:

- Data or information, whether physical or virtual; or
- Information technology resources, 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
  - Security information, whether physical or virtual, which relates to the agency's existing or proposed information technology systems.

These records are available to the Auditor General, the Division of State Technology within the department, the Cybercrime Office of the Department of Law Enforcement, and, for state agencies under the jurisdiction of the Governor, the Chief Inspector General. Such records may be made available to a local government, another state agency, or a federal agency for information technology security purposes or in furtherance of the state agency's official duties. This exemption applies to such records held by a state agency before, on, or after the effective date of this exemption. This exemption is subject to the Open Government Sunset Review Act in accordance with s. 119.15, F.S., and is repealed on October 2, 2021, unless reviewed and saved from repeal through reenactment by the Legislature.[46]

Finally, the portions of risk assessments, evaluations, external audits, and other reports of a state agency's information technology security program for the data, information, and information technology resources of the state agency which are held by a state agency are confidential and exempt from s. 119.07(1), F.S., and s. 24(a), Art. I of the State Constitution, 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
- Information technology 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 information technology systems.

Such portions of records are available to the Auditor General, the Cybercrime Office of the Department of Law Enforcement, the Division of State Technology within the department, and, for agencies under the jurisdiction of the Governor, the Chief Inspector General. Such portions of records may be made available to a local government, another state agency, or a federal agency for information technology security purposes or in furtherance of the state agency's official duties. This exemption applies to such records held by a state agency before, on, or after the effective date of this exemption. This exemption is subject to the Open Government Sunset Review Act in accordance with s. 119.15, F.S., and is repealed on October 2, 2021, unless reviewed and saved from repeal through reenactment by the Legislature.[47]

[46] Section 282.318(4)(j), F.S.
[47] Section 282.318(5), F.S.

III. Effect of Proposed Changes:

The bill amends s. 282.318, F.S., to make changes to the existing public records exemption provisions in s. 282.318(4)(j)3. and (5), F.S.

Subparagraph (4)(j)3. currently exempts from public record law records held by a state agency which identify detection, investigation, or response practices for suspected or confirmed information technology security incidents, if the disclosure of such records would facilitate unauthorized access to or the unauthorized modification, disclosure, or destruction of data or information or information technology, including specified types of information. The bill renumbers this provision as subsection (5) and adds a provision exempting the portion of records containing network schematics, hardware and software configurations, and encryption. Subsection (5) is renumbered as subsection (6) and maintains the exemption for portions of risk assessments, evaluations, external audits, and other reports of a state agency's information technology security program for the data, information, and information technology resources of the state agency, if disclosure of these records would have these same effects. Both exemptions: make the records available to the Auditor General, the Division of State Technology within the department, the Cybercrime Office of the Department of Law Enforcement, and, for state agencies under the jurisdiction of the Governor, the Chief Inspector General; make the exemption retroactive; and subject the exemption to the Open Government Sunset Review Act (OGSR).

The majority of the changes the bill makes to these two public records exemptions streamline and simplify the exemptions by deleting redundant provisions and restructuring the remaining provisions to maintain the same effect.

The bill also creates a public meetings exemption under s. 282.318(7), F.S., for those portions of a public meeting which would reveal records that the above provisions makes exempt. No exempt portion of an exempt meeting may be off the record, but must be recorded and transcribed. A recording and transcript is confidential and exempt from disclosure unless a court of competent jurisdiction, after an in camera review, determines that the meeting was not restricted to the discussion of data and information made confidential and exempt by this section. In the event of such a judicial determination, only that portion of the recording and transcript which reveals nonexempt data and information may be disclosed to a third party.

The OGSR process for the exemptions provides for an automatic repeal on October 2, 2025 unless reviewed and saved by the Legislature before then.

The bill makes a legislative finding that both public records exemptions, as amended, are a public necessity for the following reasons.

- Network schematics, hardware and software configurations, encryption, and information technology detection, investigation, or response practices for suspected or confirmed information technology security incidents or breaches are likely to be used in the investigations of the incidents or breaches. The release of portions of records held by a state agency which contain such information could impede the investigation and impair the ability of reviewing entities to effectively and efficiently execute their investigative duties. In

addition, the release of such information before an active investigation is completed could jeopardize the ongoing investigation.

- An investigation of an information technology security incident or breach is likely to result in the gathering of sensitive personal information, including identification numbers and personal financial and health information. Such information could be used to commit identity theft or other crimes. In addition, release of such information could subject possible victims of the security incident or breach to further harm.
- Disclosure of a record containing information that would reveal weaknesses in a state agency's data security, including a computer forensic analysis, could compromise that security in the future if such information were available upon conclusion of an investigation or once an investigation ceased to be active.
- Such records are likely to contain proprietary information about the security of the system at issue. The disclosure of such information could result in the identification of vulnerabilities and further breaches of that system. In addition, the release of such information could give business competitors an unfair advantage and weaken the security technology supplier supplying the proprietary information in the marketplace.
- The disclosure of such records could potentially compromise the confidentiality, integrity, and availability of state agency data and information technology resources, which would significantly impair the administration of vital state programs. It is necessary that this information be made confidential in order to protect the technology systems, resources, and data of state agencies.
- It is valuable, prudent, and critical to a state agency to have an independent entity conduct a risk assessment, an audit, or an evaluation or complete a report of the agency's information technology program or related systems. Such documents would likely include an analysis of the agency's current information technology program or systems which could clearly identify vulnerabilities or gaps in current systems or processes and propose recommendations to remedy identified vulnerabilities.

The bill makes a legislative finding of a public necessity to exempt those portions of a public meeting which would reveal data and information that the bill makes exempt from public records law, and of a public necessity to exempt the resulting recordings and transcripts, for the following reasons.

- Such meetings must be made exempt from open meetings requirements in order to protect agency information technology systems, resources, and data. This information would clearly identify a state agency's information technology systems and its vulnerabilities and disclosure of such information would jeopardize the information technology security of the state agency and compromise the integrity and availability of state agency data and information technology resources. Such disclosure would significantly impair the administration of state programs.
- It is necessary that the resulting recordings and transcripts be made confidential and exempt from public record requirements in order to protect state information technology systems, resources, and data. The disclosure of such recordings and transcripts would clearly identify a state agency's information technology systems and its vulnerabilities. This disclosure would jeopardize the information technology security of the agency and compromise the integrity and availability of state data and information technology resources, which would significantly impair the administration of state programs.

The bill also makes a legislative finding that these public meeting and public records exemptions must be given retroactive application because they are remedial in nature.

The bill takes effect upon becoming a law.

IV. Constitutional Issues:

A. Municipality/County Mandates Restrictions:

None.

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 or public meetings requirements. This bill expands an existing public records exemption to include portions of records which contain network schematics, hardware and software configurations, or encryption and creates a new public meetings exemption for the portion of a meeting at which specified exempt records are discussed. Thus, the bill requires a two-thirds vote to be enacted.

Public Necessity Statement

Article I, s. 24(c) of the State Constitution requires a bill creating or expanding an exemption to the public records or public meetings requirements to state with specificity the public necessity justifying the exemption. Section 2 of the bill contains statements of public necessity for the exemptions.

Breadth of Exemption

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 state agency data and information technology. This bill expands existing provisions to exempt only portions of records which contain network schematics, hardware and software configurations, or encryption from the public records requirements and creates a public meetings exemption to exempt only those portions of meetings discussing the information relating to state agency data and information technology security which are already exempt or made exempt by the bill. The exemptions do not appear to be broader than necessary to accomplish the purpose of the law.

C. Trust Funds Restrictions:

None.

D. State Tax or Fee Increases:

None.

E. Other Constitutional Issues:

None.

V. Fiscal Impact Statement:

A. Tax/Fee Issues:

None.

B. Private Sector Impact:

None.

C. Government Sector Impact:

None.

VI. Technical Deficiencies:

None.

VII. Related Issues:

None.

VIII. Statutes Affected:

This bill substantially amends section 282.318 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.