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:	SB 7024
INTRODUCER:	Governmental Oversight and Accountability Committee
SUBJECT:	OGSR/Cybersecurity, Information Technology, and Operational Technology Information
DATE:	January 20, 2026
REVISED:	

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

I. Summary:

SB 7024 expands the current public records and public meeting exemptions codified in s. 119.0725, F.S., which make confidential and exempt certain cybersecurity information held by state and local governmental agencies and any private entity acting on their behalf. The bill also consolidates and incorporates into s. 119.0725, F.S., from other agency-specific cybersecurity provisions the following cybersecurity-related exemptions:

- Information relating to processes or practices designed to protect data, information, or existing or proposed information technology (IT) or operational technology.
- Portions of risk assessments, evaluations, audits, and other reports of an agency's cybersecurity program.
- Login credentials.
- Internet protocol addresses, geolocation data, and other information describing how and when users access public-facing portals.
- Insurance and self-insurance coverage limits, deductibles, and other coverages acquired for the protection of IT, operational technology, or data of an agency.

The exemption in s. 119.0725, F.S., is subject to the Open Government Sunset Review Act and stands repealed on October 2, 2026, unless reenacted by the Legislature. The bill saves the exemption from repeal by delaying the scheduled repeal date, thereby maintaining the exempt status of the information until October 2, 2031. The bill also expands the public records and public meeting exemption and therefore will require a two-thirds vote.

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

The bill takes effect upon becoming a law.

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]

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]

---

[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.
[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.

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]

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]

---

[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).
[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."

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 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]

Public Records Exemptions for Cybersecurity Information

Both state and local governments are required by various Florida laws[32] to create or receive 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.[33] Additionally, the Auditor General "regularly conducts information technology audits of

[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).
[30] *Id*.
[31] *Halifax Hosp. Medical Center v. News-Journal Corp., 724 So. 2d 567 (Fla. 1999).* In *Halifax Hospital*, the Florida Supreme Court found that a public meeting 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. 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 record statute was to create a public record exemption.* The *Baker County Press* court found that since the law did not contain a public necessity statement, it was unconstitutional. *Id.* at 196.
[32] *See, e.g.*, s. 282.318, F.S.
[33] Florida Office of Inspector General, *Cybersecurity Resources*, https://www.floridaoig.com/cyberSecurity.htm (last visited Jan. 13, 2026). *See, e.g.*, Florida Department of State Office of Inspector General, *Annual Audit Plan for the 2023-2024 Fiscal Year and Long Range Plan*, (June 22, 2023), https://files.floridados.gov/media/706921/dos-oig-audit-plan-2023-24-fy.pdf (last visited Jan. 13, 2026).

governmental entities pursuant to s. 11.45, F.S."[34] Further, agencies are required to communicate incident reports and after-action reports regarding hacking events to specific governmental entities.

Agency Cybersecurity Public Records Exemption, Section 119.0725, F.S.

Section 119.0725(2), F.S., makes confidential and exempt from the public inspection and copying requirements the following cybersecurity-related information:[35]

- Coverage limits and deductible or self-insurance amounts of insurance or other risk mitigation coverages acquired for the protection of information technology (IT)[36] systems, operational technology[37] 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;
- Cybersecurity[38] incident information (whether the incident was actual or merely threatened) 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[39] 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 Florida Digital Service (FLDS), and—for agencies under the jurisdiction of the Governor—the Chief Inspector General. An agency *may* disclose the 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."[40]

---

[34] 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).
[35] Section 119.0725(2), F.S. This public records exemption was implemented in 2022, after s. 282.318, F.S., was passed, to better address ransomware incidents.
[36] "Information technology" is defined in s. 119.0725(1)(f), F.S., as "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."
[37] "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.
[38] Section 119.0725(1)(c), F.S., defines "cybersecurity" as 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.
[39] "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.
[40] Section 119.0725(5), F.S.

Agencies must still report information about cybersecurity incidents in the aggregate.[41]

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. 119.0725, F.S., was created.[42]

Section 119.0725(3), F.S., also provides 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.

The 2022 public necessity statement for s. 119.0725, F.S., provided that:

> Release of such information could place an agency at greater risk of breaches, cybersecurity incidents, and ransomware attacks … Therefore, this information should be made confidential and exempt in order to protect the agency's data, information, and information technology resources. [Furthermore,] failure to close that portion of a meeting at which confidential and exempt information would be revealed, and prevent the disclosure of the recordings and transcripts of those portions of a meeting, would defeat the purpose of the underlying public records exemption and could result in the release of highly sensitive information related to the cybersecurity of an agency system.

The public records and public meeting exemptions in s. 119.0725, F.S., will repeal on October 2, 2026, unless reenacted by the Legislature.

Section 282.318(4), F.S., Cybersecurity Public Records Exemptions

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

- Comprehensive risk assessments, whether completed by the agency itself or a private vendor;[43]
- Internal policies and procedures that, if disclosed, could facilitate the unauthorized modification, disclosure, or destruction of data or IT resources;[44] and
- The results of internal cybersecurity audits and evaluations.[45]

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.

These provisions were enacted in 1989, and the legislature was not required to set forth a public necessity statement regarding the exemption at the time.[46]

[41] Section 119.0725(6), F.S.
[42] See ch. 2022-220, Laws of Fla.
[43] Section 282.318(4)(d), F.S.
[44] Section 282.318(4)(e), F.S.
[45] Section 282.318(4)(g), F.S.
[46] *See*, ch. 89-14, Laws of Fla.

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 records inspection and copying requirements the portions of risk assessments,[47] evaluations, external audits,[48] and other reports of a state agency's cybersecurity program for the data, information, and state agency IT resources[49] 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.

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.[50]

The 2020 public necessity statement for the public records exemption created in s. 282.318(5), F.S., stated that such information was required to be held as confidential and exempt because the disclosure could impede agency investigations about breaches; result in the disclosure of sensitive personal information or proprietary business information likely to be collected during such investigation, which could facilitate identity theft or otherwise subject victims to further criminal mischief; and reveal weaknesses in a state agency's data security.

Other Cybersecurity-related Exemptions

The Legislature has enacted multiple agency-specific[51] public records and public meeting exemptions to protect cybersecurity-related information from disclosure. While these agency-specific exemptions address a similar public purpose to s. 119.0715, F.S., they are dispersed across multiple chapters of law and vary in scope and terminology. These exemptions currently protect the following information:

[47] 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."
[48] 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.
[49] Section 282.0041(22), F.S., defines "IT resources" as data processing hardware and software services, communications, supplies, personnel, facility resources, maintenance, and training.
[50] Section 282.382(7), F.S.
[51] "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, 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. Section 119.011(2), F.S.

- Secure login credentials and related security information held by the Department of State (DOS) relating to certain password-protected systems.[52]
- Information relating to the Department of the Lottery's cybersecurity technologies, processes, and practices designed to protect its IT systems and data.[53]
- User identifications and passwords held by DOS relating to the electronic filing system for campaign finance reports.[54]
- Secure login credentials held by the Commission on Ethics relating to the electronic filing system for financial interest disclosures.[55]
- Sensitive agency-produced data processing software.[56]
- Secure login credentials, Internet protocol addresses, geolocation data, and other information that describes the location, computer, computer system, or computer network from which a user accesses a public-facing portal, and the dates and times that a user accesses a public-facing portal, held by the Department of Highway Safety and Motor Vehicles.[57]
- Information relating to a utility's (that is owned or operated by a unit of local government) security processes and practices designed to protect its IT or industrial control technology systems.[58]
- Cybersecurity policies and procedures, audits, risk assessments, evaluations, and other reports of a state agency's cybersecurity program.[59]
- Risk assessments, evaluations, audits, and other reports of Citizens Property Insurance Corporation's cybersecurity program.[60]
- Information identifying detection, investigation, or response practices, and risk assessments, evaluations, audits, and other reports, relating to the cybersecurity program of a state university or Florida College System Institution.[61]

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,[62] with specified exceptions.[63] 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.[64] In practice, many exemptions are continued by repealing the sunset date, rather than reenacting the exemption.

[52] Section 15.16(3)(c)2., F.S.
[53] *See* s. 24.1051(1)(a)1.a., F.S.
[54] Section 106.0706(1), F.S.
[55] Section 112.31446(6)(a), F.S.
[56] Section 119.071(1)(f), F.S. This exemption currently applies to all agencies.
[57] Section 119.0712(2)(f), F.S.
[58] *See* s. 119.0713(5)(a)1.-2., F.S.
[59] *See* s. 282.318(4)-(9), F.S.
[60] Section 627.352, F.S.
[61] *See* s. 1004.055, F.S.
[62] 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.
[63] 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.
[64] Section 119.15(3), F.S.

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.[65] An exemption serves an identifiable purpose if the Legislature finds that the purpose of the 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;[66]
- 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;[67] or
- It protects trade or business secrets.[68]

The Act also requires specified questions to be considered during the review process.[69] Of particular importance to this review is the question of whether there are multiple exemptions for the same type of record that it would be appropriate to merge. 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.[70] 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.[71]

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

In order to allow these two cybersecurity exemptions to be reviewed concurrently, the Legislature delayed the originally scheduled 2025 repeal of the cybersecurity public records and meeting exemption in s. 282.318(5)-(6), F.S., for one year, setting the new repeal date for October 2, 2026. Conversely, the Legislature moved up by one year (from October 2, 2027, to October 2, 2026), the Open Government Sunset Review for the public records and public meeting exemptions in s. 119.0725(2) and (3), F.S.[72]

---

[65] Section 119.15(6)(b), F.S.
[66] Section 119.15(6)(b)1., F.S.
[67] Section 119.15(6)(b)2., F.S.
[68] Section 119.15(6)(b)3., F.S.
[69] 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?

[70] FLA. CONST. art. I, s. 24(c).
[71] Section 119.15(7), F.S.
[72] Ch. 2025-27, Laws of Fla.

The staff of the Senate Governmental Oversight and Accountability Committee and the House Government Operations Subcommittee subsequently surveyed Florida agencies to ascertain whether the public records and open meeting exemptions in ss. 282.318(5) and (6), 119.0725, and 119.0712(2)(f), F.S., remain necessary. Staff reviewed a total of 172 agency responses, a majority of which recommend that the Legislature reenact the public records exemptions without any changes.

Public Records and Meeting Exemption Findings

As part of the questionnaire, respondents were asked whether any agency-specific cybersecurity exemption should be incorporated into the general cybersecurity exemption. Some respondents suggested merging agency-specific exemptions into the general exemption, while others suggested maintaining the status quo.

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, 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.[73] As outlined above, there are at least three public records exemptions that may cover information made confidential and exempt by s. 119.0725, F.S. Several agencies seem to rely on the exemptions as a group to protect "cybersecurity information" rather than distinguish between them.

III. Effect of Proposed Changes:

Removal of Schedule Repeal of Public Records and Meeting Exemptions

The public records and public meeting exemptions for cybersecurity-related information in ss. 119.0712(2), 119.0725(2)(h), and 282.3185(5)-(6), F.S., will repeal on October 2, 2026, if this bill does not become law.

The bill maintains the confidential and exempt status of specific cybersecurity information held by an agency, and its associated public meeting exemption, by delaying the scheduled repeal date in s. 119.0725, thereby maintaining the exempt status of the information until October 2, 2031.

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

Section 1 amends s. 119.0725, F.S., to remove the scheduled repeal date for the public records exemption for cybersecurity information held by an agency, and the public meeting exemption for any portion of a meeting that would reveal such confidential and exempt cybersecurity information (as well as its associated public records exemption for the recording and transcript of such exempt portions of meetings). This information will maintain its confidential and exempt status.

Rather than remove the scheduled repeal date and continue the public records exemption provided for in s. 119.0712(2) and the public records and meeting exemptions provided for in s. 282.3185(5)-(6), F.S., **sections 9 and 12** delete the entirety of those cybersecurity exemptions. These provisions were found appropriate to merge with the cybersecurity exemption in s. 119.0725, F.S., which is saved from repeal by this bill. The substance of sections 9 and 12 are discussed further below.

Expansion of Agency Cybersecurity Public Records Exemption

Section 1 amends s. 119.0725, F.S., to expand the general agency public records exemption for cybersecurity[74] information to include the following categories of information:

- Network schematics, hardware and software configurations, encryption information, or information identifying detection, investigation, or response practices related to cybersecurity incidents,[75] including breaches,[76] if disclosure could facilitate unauthorized access to or unauthorized modification, disclosure, or destruction of data, information, or existing or proposed IT or operational technology.
- Information relating to processes or practices designed to protect data, information, or existing or proposed IT or operational technology if disclosure could facilitate unauthorized access to or unauthorized modification, disclosure, or destruction of such data, information, or technology.
- Portions of risk assessments, evaluations, audits, and other reports of an agency's cybersecurity program if disclosure could facilitate unauthorized access to or unauthorized modification, disclosure, or destruction of data, information, or existing or proposed IT or operational technology.
- Login credentials.[77]
- Internet protocol addresses, geolocation data, and other information that describes the location, computer, computer system, or computer network from which a user accesses a public-facing portal,[78] and the dates and times that a user accesses a public-facing portal.

[74] The bill defines "cybersecurity" to mean the protection afforded to IT and operational technology in order to attain the applicable objectives of preserving the confidentiality, integrity, and availability of those technologies, data, and information.
[75] The bill defines "incident" to mean a violation or imminent threat of violation, whether such violation is accidental or deliberate, of an agency's cybersecurity, IT, or operational technology.
[76] The bill defines "breach" to mean unauthorized access of data or information. Good faith access of data or information by an employee or agent of an agency does not constitute a breach, provided that the data or information is not used for a purpose unrelated to the business or subject to further unauthorized use.
[77] The bill defines "login credentials" to mean information used to authenticate a user's identity or otherwise access when logging into a computer, computer system, computer network, electronic device, or an online user account accessible over the Internet through a mobile device, a website, or any other electronic means, or for authentication or password or account recovery.
[78] The bill defines a "public-facing portal" as a web portal or computer application that is publicly accessible over the Internet, via mobile device, website, or other electronic means.

- Sensitive agency-produced data processing software.
- Insurance and self-insurance coverage limits and deductibles, and other risk mitigation coverages, acquired for the protection of IT, OT, or data of an agency.

The bill allows an agency to disclose the above confidential and exempt information in furtherance of its official duties and responsibilities, or to another agency or governmental entity in the furtherance of their official duties and responsibilities. This is an expansion from prior language, which allowed an agency to request such information in furtherance of its statutory duties.

The bill republishes the public meeting exemption associated with the public records exemption codified in s. 119.0725, F.S,, thereby expanding the public meeting exemption to include the material added in the underlying public records exemption as described above.

The bill provides that the exemptions apply to information held by an agency before, on, or after the effective date of the act. The public records and public meeting exemptions will automatically repeal on October 2, 2031, unless reviewed and saved from repeal by the Legislature.

Section 15 provides the public necessity statement required by article I, section 24(c) of the State Constitution for the expansion of the public records and meeting exemptions. The statement provides a finding that the release of the specific cybersecurity information could place an agency at greater risk of breach, incident, and ransomware attack. The disclosure of such information could provide bad actors with knowledge about IT and operational technology structures, defenses, and vulnerabilities, making agency operations subject to malicious actions.

The release of login credentials and other security-related information (such as user location) would similarly provide bad actors with methods to access agency IT and operational systems, thus making agency information and systems subject to harm.

Lastly, public knowledge of an agency's cybersecurity insurance could provide cybercriminals with an understanding of the limits of an agency's willingness to pay as a result of a ransomware attack.

All of these vulnerabilities based on the exposure of cybersecurity-related agency information (as either a record, or at a meeting) would result in an expense to taxpayers, and impairment of vital government programs.

Transfer of Agency-Specific Cybersecurity Exemptions

Sections 2-3, 5-6, 9-10 and 12-14 delete agency-specific public records cybersecurity exemptions that are made duplicative by the transfer of their exemptions to the broader agency cybersecurity exemption codified in s. 119.0725, F.S.

Section 2 amends s. 15.16, F.S., to delete a public records exemption for secure login credentials and related information held by the Department of State for the purpose of allowing a person to

electronically file records. The substance of this exemption is transferred to s. 119.0725, F.S., by section 1 of the bill, to apply to all governmental agencies.

Section 3 amends s. 24.1051, F.S., to delete a public records exemption for information relating to the Department of the Lottery's cybersecurity technologies, processes, and practices designed to protect its IT systems and data.

Section 5 amends s. 106.0706, F.S., to delete a duplicative exemption for user identifications and passwords held by DOS relating to the electronic filing system for campaign finance reports.

Section 6 amends s. 112.31446, F.S., to delete a now-duplicative exemption for secure login credentials held by the Commission on Ethics relating to the electronic filing system for financial interest disclosures.

Section 9 amends s. 119.0712, F.S., to delete a now-duplicative exemption for secure login credentials, Internet protocol addresses, geolocation data, and other information that describes the location, computer, computer system, or computer network from which a user accesses a public-facing portal, and the dates and times that a user accesses a public-facing portal, held by the Department of Highway Safety and Motor Vehicles.

Section 10 amends s. 119.0713, F.S., to delete a now-duplicative exemption for information relating to a utility's (that is owned or operated by a unit of local government) security processes and practices designed to protect its IT or industrial control technology systems.

Section 12 amends s. 282.318, F.S., to delete a now-duplicative exemption for cybersecurity policies and procedures, audits, risk assessments, evaluations, and other reports of a state agency's cybersecurity program.

Section 13 repeals s. 627.352, F.S., which makes confidential and exempt from public records inspection and copying requirements any risk assessments, evaluations, audits, and other reports of Citizens Property Insurance Corporation's cybersecurity program. The substance of this exemption is transferred to s. 119.0725, F.S.

Section 14 repeals s. 1004.055, F.s., which makes confidential and exempt information that identifies detection, investigation, or response practices, and risk assessments, evaluations, audits, and other reports, that relate to the cybersecurity program of a state university or Florida College System Institution.

Update of Cross-References

Section 8 deletes a public records exemption for agency-produced data processing software that is sensitive and instead incorporates it into s. 119.0725, F.S. **Sections 4, 7, and 11** update cross-references to s. 119.071(1)(f), F.S., in ss. 101.5607, 119.07, and s. 119.0714, F.S., respectively to reflect the transfer of the exemption to s. 119.0725(2)(h), F.S.

Effective Date

The bill takes effect upon becoming a law.

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 expands the current public records exemption and public meeting exemption; thus, the bill requires 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 expands a current public records and public meeting exemption and therefore requires a new public necessity statement. Section 15 of the bill meets that requirement, noting the release of the cybersecurity-related information protected by the bill could place Florida's agencies at greater risk of breaches, cybersecurity incidents, and ransomware attacks, thereby impairing the administration of vital government programs and result in greater expense to taxpayers.

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 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 records request for information covered by s. 119.0725, 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. Agencies may see efficiency is training as a result of the condensing of cybersecurity-related exemptions into one section of law.

VI. Technical Deficiencies:

None.

VII. Related Issues:

Section 119.0714, F.S., excludes information made part of a court file from the exemptions provided for in ch. 119, F.S., except those documents specifically closed by a court or specifically listed in law, including sensitive data processing software that is produced by an agency.

Florida courts have consistently held that the judiciary is not an "agency" for purposes of ch. 119, F.S. However, art. I, s. 34 of the State Constitution still provides a constitutional right of access to judicial records. In order to balance the separation of powers between the legislative and judicial branches, confidentiality of court records is governed by court rule and court decisions. Florida Rule of General Practice and Judicial Administration 2.420, entitled "Public Access to and Protection of Judicial Branch Records", provides that "the public shall have access to all records of the judicial branch of government except as provided [in the rule]."

The court system adopts its own exemptions regarding public records, and there will likely be a delay between the effective date of this bill and any update to court rules regarding the confidentiality of sensitive data processing software produced by an agency. However, since the

needed update is limited to a technical cross-reference, rather than a substantive change of the subject of confidentiality—there should be no actual loss of confidentiality between that time.

VIII. Statutes Affected:

This bill substantially amends the following sections of the Florida Statutes: 119.0725, 15.16, 24.1051, 101.5607, 106.0706, 112.31446, 119.07, 119.071, 119.0712, 119.0713, 119.0714, and 282.318.

This bill repeals the following sections of the Florida Statutes: 627.352 and 1004.055, F.S.

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.