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 Rules

BILL:	CS/SB 7042
INTRODUCER:	Rules Committee; Banking and Insurance Committee
SUBJECT:	OGSR/Citizens Property Insurance Corporation
DATE:	April 20, 2023 REVISED:

	ANALYST	STAFF DIRECTOR	REFERENCE	ACTION
	Moody	Knudson		**BI Submitted as Committee Bill**
1.	Moody	Twogood	RC	**Fav/CS**

Please see Section IX. for Additional Information:

COMMITTEE SUBSTITUTE - Substantial Changes

I. Summary:

CS/SB 7042 repeals s. 627.352(1)(a), F.S., which makes confidential and exempt from disclosure records held by the Citizens Property Insurance Corporation (Citizens) which identify detection, investigation, or response practices for suspected or confirmed information technology security incidents if certain criteria are met.

The bill saves from repeal the public records exemption in s. 627.352(1)(b), F.S., maintaining the exemptions in current law for any portions of a risk assessment, an evaluation, an audit, and any other reports of Citizens' information technology security program for its data, information, and information technology resources which are held by Citizens, if the disclosure meets certain criteria.

The bill makes technical amendments, including clarifying that "confidential and exempt" records and portions of public meeting records and transcripts are available to certain entities.

The public records exemption stands repealed on October 2, 2023, unless reviewed and reenacted by the Legislature under the Open Government Sunset Review Act. The bill removes the scheduled repeal of the exemption to continue the confidential and exempt status of the information under s. 627.352(1)(b), F.S.

This bill is not expected to impact state or local government revenues or expenditures.

The bill is effective October 1, 2023.

II. Present Situation:

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 who acts on behalf of the government.[2]

Chapter 119, F.S., known as the Public Records Act, constitutes the main body of public records laws.[3] The Public Records Act states that:

> [i]t is the policy of this state that all state, county, and municipal records are open for personal inspection and copying by any person. Providing access to public records is a duty of each agency.[4]

The Public Records Act contains general exemptions that apply across agencies. Agency- or program-specific exemptions often are placed in the substantive statutes that relate to that particular agency or program.

The Public Records Act does not apply to legislative or judicial records.[5] 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.

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 connections 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

[1] FLA. CONST., art. I, s. 24(a).
[2] *Id*.
[3] Public records laws are found throughout the Florida Statutes.
[4] Section 119.01(1), F.S.
[5] *Locke v. Hawkes*, 595 So. 2d 32, 34 (Fla. 1992); *see also, Times Pub. Co. v. Ake*, 660 So. 2d 255 (Fla. 1995).
[6] *Shevin v. Byron, Harless, Schaffer, Reid and Assoc. Inc*., 379 So. 2d 633, 640 (Fla. 1980).

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 which justifies the exemption.[10] Further, the exemption must be no broader than necessary to accomplish the stated purpose of the law. A bill that enacts 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]

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,[16] with specified exceptions.[17] 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.[18] 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. 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:

---

[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).
[16] 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.
[17] 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.
[18] Section 119.15(3), F.S.

- It allows the state or its political subdivision to effectively and efficiently administer a program, and administration would be significantly impaired without the exemption;[19]
- The release of sensitive personal information 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;[20] or
- It protects trade or business secrets.[21]

The Act also requires specified questions to be considered during the review process.[22] In examining an exemption, the Act directs the Legislature to question the purpose and necessity of reenacting the exemption.

If, in reenacting an exemption or repealing the sunset date, the exemption is expanded, then a public necessity statement and a two-thirds vote for passage are required.[23] 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.[24]

Current State Agency Cybersecurity Information Exemptions

The State Cybersecurity Act provides for statutory exemptions of public records disclosure by state agencies related to information technology that are contained in s. 282.318(5) through (10), F.S. Similar statutory exemptions for utilities owned or operated by local governments are provided in s. 119.0713(5), F.S.

Portions of risk assessments, evaluations, external audits,[25] and other reports of a state agency's cybersecurity[26] program for the data, information, and information technology resources of the state agency[27] which are held by a state agency are confidential and exempt if the disclosure

[19] Section 119.15(6)(b)1., F.S.
[20] Section 119.15(6)(b)2., F.S.
[21] Section 119.15(6)(b)3., F.S.
[22] Section 119.15(6)(a), F.S. The specific 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?

[23] FLA. CONST. art. I, s. 24(c).
[24] Section 119.15(7), F.S.
[25] Section 282.318(5), F.S., defines "external audit" as an audit that is conducted by an entity other than the state agency that is the subject of the audit.
[26] Section 282.0041(8), 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.
[27] Section 282.0041(34), F.S., defines "state agency" as any official, officer, commission, board, authority, council, committee, or department of the executive branch of state government; the Justice Administrative Commission; and the Public Service Commission. The term does not include the Department of Legal Affairs, The Department of Agriculture and

would facilitate unauthorized access to or the unauthorized modification, disclosure, or destruction of:

- Data[28] or information, whether physical or virtual; or
- Information technology (IT) resources,[29] 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 IT[30] systems.[31,32]

In addition, any portion of a public meeting that would reveal any of the above-described confidential and exempt records is exempt from public meeting requirements. Any portion of an exempt meeting must be recorded and transcribed. The recordings and transcripts are confidential and exempt from public record requirements unless a court of competent jurisdiction, following an in camera review, determines that the meeting was not restricted to the discussion of confidential and exempt data and information. If such a judicial determination occurs, only the portion of the recording or transcript that reveals nonexempt data may be disclosed.[33]

The confidential and exempt cybersecurity information must be available to the Auditor General, the Cybercrime Office within the Florida Department of Law Enforcement (FDLE), the Florida Digital Service (FLDS),[34] and for agencies under the jurisdiction of the Governor, the Chief Inspector General. In addition, the records may be made available to a local government, another state agency, or a federal agency for cybersecurity purposes or in the furtherance of the state agency's official duties.[35]

Consumer Services, and the Department of Financial Services. The term does not include university boards of trustees or state universities.

[28] Section 282.0041(9), F.S., defines "data" as a subset of structured information in a format that allows such information to be electronically retrieved and transmitted.

[29] Section 119.011(9), F.S., defines "information technology resources" as data processing hardware and software and services, communications, supplies, personnel, facility resources, maintenance, and training.

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

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

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

[33] Section 282.318(6), F.S. Florida law provides a similar public meeting exemption for state university and Florida College system institutions, see s. 1004.055, F.S.

[34] Section 20.22(2)(b), F.S., provides that Florida Digital Service (FLDS) (formerly the Division of State Technology) is a subdivision of the Department of Management Services (DMS) and is charged with overseeing the state's information technology (IT) resources.

[35] Section 282.318(7), F.S.

Information related to the security of a utility[36] owned or operated by a unit of local government[37] that is designed to protect the utility's networks, computers, programs, and data from attack, damage or unauthorized access, is exempt from public record requirements to the extent disclosure of such information would facilitate the alteration, disclosure, or destruction of data or IT resources.[38]

In addition, information related to the security of existing or proposed IT systems or industrial control technology systems of a utility owned or operated by a unit of local government is exempt from public record requirements to the extent disclosure would facilitate unauthorized access to, and the alternation or destruction of, such IT systems in a manner that would adversely impact the safe and reliable operations of the IT systems and the utility.[39]

Exemptions Related to Agency Cybersecurity Information

In 2022, the Legislature adopted public records and public meetings exemptions for agency cybersecurity information under s. 119.0725, F.S.[40] The new section makes the following information held before, on, or after July 1, 2022 by an agency[41] confidential and exempt from public disclosure requirements under ch. 119, F.S.,:

- Coverage limits and deductible or self-insurance amounts of insurance or other risk mitigation coverages acquired for the protection of IT systems, operational technology (OT) systems,[42] or data of an agency.
- Information relating to critical infrastructure.[43]
- Network schematics, hardware and software configurations, or encryption information or information that identifies detection, investigation, or response practices for suspected or confirmed cybersecurity incidents, including suspected or confirmed breaches,[44] if the disclosure of such information would facilitate unauthorized access to or unauthorized modification, disclosure, or destruction of:
  - Data or information, whether physical or virtual; or
  - IT resources, which include an agency's existing or proposed IT systems.

[36] Section 119.011(15), F.S., defines "utility" as a person or entity that provides electricity, natural gas, telecommunications, water, chilled water, reuse water, or wastewater.
[37] Section 119.0713(2)(a), F.S., defines "unit of local government" as a county, municipality, special district, local agency, authority, consolidated city -county government, or any other local governmental body or public body corporate or politic authorized or created by general or special law.
[38] Section 119.0713 (5)(a)1., F.S.
[39] Section 119.0713(5)(a)2., F.S.
[40] Ch. 2022-221, L.O.F.
[41] 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.
[42] Section 119.0725(1)(g), F.S., defines "operational technology" as the hardware and software that cause or detect a change through the direct monitoring or control of physical devices, systems, processes, or events.
[43] Section 119.0725(1)(b), F.S., defines "critical infrastructure" as existing and proposed information technology and operational technology systems and assets, whether physical or virtual, the incapacity or destruction of which would negatively affect security, economic security, public health, or public safety.
[44] Section 119.0725(1)(a), F.S., defines "breach" as unauthorized access of data in electronic form containing personal information. Good faith access of personal information by an employee or agent of an agency does not constitute a breach, provided that the information is not used for a purpose unrelated to the business or subject to further unauthorized use.

- Cybersecurity incident information reported pursuant to Sections 282.318 or 282.3185, F.S.

Any portion of a meeting that would reveal information made confidential and exempt under s. 119.0725(2), F.S., is exempt from public meeting disclosure requirements; however, any portion of an exempt meeting must be recorded and transcribed. The recording and transcript are confidential and exempt from public record requirements.[45]

Such confidential and exempt information may to be made available to:

- A law enforcement agency.
- The Auditor General.
- The Cybercrime Office within FDLE.
- The Florida Digital Service.
- For agencies under the jurisdiction of the Governor, the Chief Inspector General.[46]

Further, confidential and exempt information is authorized to be released:

- In the furtherance of the custodial agency's duties and responsibilities; or
- To another governmental entity in the furtherance of its statutory duties and responsibilities.[47]

Agencies are authorized to report information about cybersecurity incidents in an aggregate format.[48]

Section 119.0725, F.S., provides for repeal of the exemptions on October 2, 2027, unless reviewed and saved from repeal through reenactment of the Legislature.

Citizens Property Insurance Corporation

Citizens is a state-created, not-for-profit, tax-exempt governmental entity whose mission is to provide property insurance coverage to those unable to find affordable coverage in the private market.[49] It is not a private insurance company.[50]

Records and meetings held by Citizens regarding information security incidents, such as investigations into security breaches, security technologies, processes and practices as well as security risk assessments are subject to Florida open records and meetings laws. Public disclosure of this information presents a significant security risk and would reveal weaknesses within Citizens' computer networks, raising the potential for exploitation.

Because Citizens is not created within the executive branch, it is not covered by the definition of "state agency"[51] contained in the State Cybersecurity Act. Accordingly, Citizens is not subject to

[45] Section 119.0725(3), F.S.
[46] Section 119.0725(5)(a), F.S.
[47] Section 119.0725(5)(b), F.S.
[48] Section 119.0725(6), F.S.
[49] *See* Citizens Property Insurance Corporation, Who We Are, available at https://www.citizensfla.com/who-we-are (last viewed on March 6, 2023). *See also* s. 627.351(6)(a), F.S.
[50] Section 627.351(6)(a)1., F.S.
[51] *See supra* note 27.

the exemptions from open meetings and public records laws for data and information technology systems owned, contracted, or maintained by specified state agencies. Therefore, Citizens is vulnerable to the disclosure of such information and records which, if disclosed, could potentially compromise the confidentiality, integrity, and availability of its information technology system. Such system contains highly sensitive policyholder, insurer, claims, financial, accounting and banking, personnel, and other records.[52]

Citizens does fall within the definition of "agency" under s. 119.011(2), F.S., and, therefore, cybersecurity information that is subject to the public records and public meetings exemptions under s. 119.0725, F.S., apply to Citizens.

Security of Data and Information Technology in Citizens Property Insurance Corporation

Section 627.352, F.S., provides for a public record and public meeting exemptions to protect data and records pertaining to the security of the Citizens information networks from disclosure. Records held by Citizens that identify detection, investigation, or response practices for suspected or confirmed IT security incidents, including suspected or confirmed breaches, are confidential and exempt from public record requirements. In addition, portions of risk assessments, evaluations, audits, and other reports of Citizens' IT security program for its data, information, and IT resources that are held by Citizens are confidential and exempt. Such records, and portions thereof, are only confidential and exempt if disclosure would facilitate unauthorized access to or unauthorized modification, disclosure, or destruction of:

- Physical or virtual data or information; or
- IT resources, including:
  - Information relating to the security of Citizens' technologies, processes, and practices designed to protect networks, computers, data processing software, and data from attack, damage, or unauthorized access; or
  - Physical or virtual security information that relates to Citizens' existing or proposed IT systems.

Section 627.352, F.S., also provides for a public meeting exemption for meetings and portions thereof that would reveal the above-described IT security information. Recordings or transcripts of such closed portions of meetings must be taken. Recordings or transcripts are confidential and exempt from public record requirements, unless a court, following an in-camera review, determines that the meeting was not restricted to the discussion of confidential and exempt data and information. In the event of such a judicial determination, only that portion of a transcript that reveals nonexempt data and information may be disclosed to a third party.

Confidential and exempt records related to the public meeting exemption are available to the Auditor General, the Cybercrime Office of Department of Law Enforcement, and the Office of Insurance Regulation. Such records and portions of meetings, recordings, and transcripts may

[52] Section 627.351(6)(x), F.S., requires Citizens to hold the following records as confidential and exempt from disclosure under Florida's public record laws: underwriting files, claim files, certain audit files, attorney-client privileged material, certain proprietary information licensed to Citizens, employee assistance program information, information relating to the medical condition or medical status of a Citizens employee, certain information relating to contract negotiations, and certain records related to closed meetings.

also be available to a state or federal agency for security purposes or in furtherance of the agency's official duties.[53]

The public record exemptions apply to records or portions of public meetings, recordings, and transcripts held by Citizens. The public records exemption applies retroactively.

This section is subject to the OGSR in accordance with s. 119.15, F.S., and stands repealed on October 2, 2023, unless reviewed and saved from repeal through reenactment by the Legislature.

III. Effect of Proposed Changes:

Section 1 repeals s. 627.352(1)(a), F.S., which makes confidential and exempt from disclosure records held by the Citizens which identify detection, investigation, or response practices for suspected or confirmed information technology security incidents, including suspected or confirmed breaches, if the disclosure would facilitate unauthorized access to or unauthorized modification, disclosure, or destruction of:

- Data or information, whether physical or virtual; or
- Information technology resources, including:
    - Information relating to the security of the corporation'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 corporation's existing or proposed information technology systems.

The confidential and exempt records protected from disclosure under s. 627.352(1)(a), F.S., are considered to fall within the scope, and therefore are duplicative, of the general exemption for agency cybersecurity information under s. 119.0725, F.S.

The bill saves from repeal the public records exemption in s. 627.352(1)(b), F.S., maintaining the exemptions in current law for any portions of a risk assessment, an evaluation, an audit, and any other reports of Citizens' information technology security program for its data, information, and information technology resources which are held by Citizens, if the disclosure would facilitate unauthorized access to or the unauthorized modification, disclosure, or destruction of:

- Data or information, whether physical or virtual; or
- Information technology resources, including:
    - Information relating to the security of the corporation'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 corporation's existing or proposed information technology systems.

Notwithstanding the similar protections provided in s. 282.318(5), F.S., this paragraph is not covered under that section because Citizens does not fall within the definition of "agency" under s. 282.0041(34), F.S.

[53] Section 627.352(3), F.S.

The bill makes technical amendments, including clarifying that "confidential and exempt" records and portions of public meeting records and transcripts are available to certain entities.[54]

The public records exemption stands repealed on October 2, 2023, unless reviewed and reenacted by the Legislature under the Open Government Sunset Review Act. The bill removes the scheduled repeal of the exemption to continue the confidential and exempt status of the information under s. 627.352(1)(b), F.S.

Section 2 provides an effective date of October 1, 2023.

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:

Voting Requirements

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 requirements. This bill does not create or expand an exemption, thus, the bill does not require 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 requirements to state with specificity the public necessity justifying the exemption. This bill does not create or expand an exemption, thus, a statement of public necessity is not required.

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 exemption in the bill does not appear to be broader than necessary to accomplish the purpose of the law.

C. Trust Funds Restrictions:

None.

[54] Section 627.352(4), F.S.

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 sections 627.352 of the Florida Statutes.

IX. Additional Information:

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

CS by Rules on April 19, 2023:
The committee substitute:

- Repeals s. 627.352(1)(a), F.S., that makes confidential and exempt records held by Citizens for suspected IT security incidents; and
- Makes technical amendments.

B. Amendments:

None.