

HOUSE OF REPRESENTATIVES STAFF ANALYSIS

BILL #: CS/CS/HB 1127 Pub. Rec. and Meetings/Citizens Property Insurance Corporation

SPONSOR(S): Government Accountability Committee; Oversight, Transparency & Administration Subcommittee; Lee, Jr.

TIED BILLS: **IDEN./SIM. BILLS:** CS/CS/SB 1880

| REFERENCE | ACTION | ANALYST | STAFF DIRECTOR or BUDGET/POLICY CHIEF |
|--|------------------|----------|---------------------------------------|
| 1) Oversight, Transparency & Administration Subcommittee | 13 Y, 0 N, As CS | Moore | Harrington |
| 2) Insurance & Banking Subcommittee | 14 Y, 0 N | Peterson | Luczynski |
| 3) Government Accountability Committee | 22 Y, 0 N, As CS | Moore | Williamson |

SUMMARY ANALYSIS

The Information Technology (IT) Security Act requires the Agency for State Technology and state agency heads to meet certain requirements relating to IT security. The act provides public record exemptions for certain information related to state agency IT security.

The bill creates public record exemptions for Citizens Property Insurance Corporation (Citizens) that are similar to those currently in law for state agencies. The bill provides that 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.

The bill also creates a public meeting exemption for meetings and portions thereof that would reveal the above-described IT security information.

The public record exemptions are retroactive and apply to records held by Citizens before, on, or after the effective date of the bill.

The bill provides for repeal of the exemptions on October 2, 2023, unless reviewed and saved from repeal through reenactment by the Legislature. The bill provides a public necessity statement as required by the State Constitution.

The bill may have a minimal fiscal impact on the state. See Fiscal Comments section.

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 newly created or expanded public record or public meeting exemption. The bill creates new public record and public meeting exemptions; thus, it requires a two-thirds vote for final passage.

This document does not reflect the intent or official position of the bill sponsor or House of Representatives.

STORAGE NAME: h1127e.GAC

DATE: 2/14/2018

FULL ANALYSIS

I. SUBSTANTIVE ANALYSIS

A. EFFECT OF PROPOSED CHANGES:

Background

Public Records Law

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

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

Public Meetings Law

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

Public policy regarding access to government meetings is also addressed in the Florida Statutes. Section 286.011, F.S., known as the "Government in the Sunshine Law" or "Sunshine Law," further requires all meetings of any board or commission of any state agency or authority or of any agency or authority of any county, municipal corporation, or political subdivision at which official acts are to be taken to be open to the public at all times. The board or commission must provide reasonable notice of all public meetings.¹ Minutes of a public meeting must be promptly recorded and be open to public inspection.²

No resolution, rule, or formal action is considered binding unless action is taken or made at a public meeting.³ Acts taken by a board or commission in violation of this requirement are considered void,⁴ though a failure to comply with open meeting requirements may be cured by independent final action by the board or commission fully in compliance with public meeting requirements.⁵

Public Record and Public Meeting Exemptions

Article I, s. 24(c) of the State Constitution authorizes the Legislature to provide by general law for the exemption of records and meetings from the requirements of Art. I, s. 24(a) and (b) of the State Constitution. The general law must state with specificity the public necessity justifying the exemption (public necessity statement) and must be no broader than necessary to accomplish its purpose.

The Open Government Sunset Review Act⁶ further provides that a public record or a public meeting exemption may be created or maintained only if it serves an identifiable public purpose. In addition, it may be no broader than is necessary to meet one of the following purposes:

- Allow the state or its political subdivisions to administer effectively and efficiently a governmental program, which administration would be significantly impaired without the exemption.

¹ Section 286.011(1), F.S.

² Section 286.011(2), F.S.

³ Section 286.011(1), F.S.

⁴ *Grapski v. City of Alachua*, 31 So. 3d 193 (Fla. 1st DCA 2010).

⁵ *Finch v. Seminole County School Board*, 995 So. 2d 1068 (Fla. 5th DCA 2008).

⁶ See s. 119.15, F.S.

- Protect sensitive personal information that, if released, would be defamatory or would jeopardize an individual's safety; however, only the identity of an individual may be exempted under this provision.
- Protect trade or business secrets.⁷

The Open Government Sunset Review Act requires the automatic repeal of a newly created exemption on October 2nd of the fifth year after creation or substantial amendment, unless the Legislature reenacts the exemption.⁸

Public Record Exemptions Related to Information Technology

The Information Technology (IT) Security Act⁹ requires the Agency for State Technology (AST) and state agency¹⁰ heads to meet certain requirements relating to IT security. The IT Security Act provides that the following state agency information is confidential and exempt¹¹ from public record requirements:

- Comprehensive risk assessments;¹²
- Internal policies and procedures that, if disclosed, could facilitate the unauthorized modification, disclosure, or destruction of data or information technology (IT) resources;¹³ and
- The results of internal audits and evaluations.¹⁴

Such confidential and exempt information must be disclosed to the Auditor General, the Cybercrime Office within the Department of Law Enforcement (DLE), AST, and, for agencies under the jurisdiction of the Governor, the Chief Inspector General.¹⁵

In addition, the IT Security Act provides that records held by a state agency that identify detection, investigation, or response practices for suspected or confirmed IT security incidents, including suspected or confirmed breaches, are confidential and exempt.¹⁶ Portions of risk assessments, evaluations, external audits, and other reports of a state agency's IT security program for the data, information, and IT resources of the state agency that are held by a state agency are confidential and exempt from public record requirements.¹⁷ Such records, and portions thereof, are only confidential and exempt if disclosure would facilitate the unauthorized access to or the unauthorized modification, disclosure, or destruction of:

- Physical or virtual data or information; or
- IT resources, including:

⁷ Section 119.15(6)(b), F.S.

⁸ Section 119.15(3), F.S.

⁹ Section 282.318, F.S.

¹⁰ The term "state agency" means any official, officer, commission, board, authority, council, committee, or department of the executive branch of state government; the Justice Administrative Commission; and the Public Service Commission. The term does not include university boards of trustees or state universities. As used in part I of this chapter, except as otherwise specifically provided, the term does not include the Department of Legal Affairs, the Department of Agriculture and Consumer Services, or the Department of Financial Services. Section 282.0041(23), F.S.

¹¹ There is a difference between records the Legislature designates exempt from public records requirements and those the Legislature deems confidential and exempt. A record classified as exempt from public disclosure may be disclosed under certain circumstances. *See Williams v. City of Minneola*, 575 So. 2d 683, 687 (Fla. 5th DCA 1991) *review denied*, 589 So. 2d 289 (Fla. 1991). If the Legislature designates a record as confidential and exempt from public disclosure, such record may not be released by the custodian of public records to anyone other than the persons or entities specifically designated in statute. *See WFTV, Inc. v. Sch. Bd. of Seminole Cnty*, 874 So. 2d 48, 53 (Fla. 5th DCA 2004), *review denied*, 892 So. 2d 1015 (Fla. 2004); *Op. Att'y Gen. Fla. 85-692* (1985).

¹² Section 282.318(4)(d), F.S.

¹³ Section 282.318(4)(e), F.S.

¹⁴ Section 282.318(4)(g), F.S.

¹⁵ Section 282.318(4)(d), (e), and (g), F.S.

¹⁶ Section 282.318(4)(i), F.S.

¹⁷ Section 282.318(5), F.S.

- Information relating to the security of the state agency’s 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 the state agency’s existing or proposed IT systems.¹⁸

Such confidential and exempt records, and portions thereof, must be made available to the Auditor General, the Cybercrime Office within DLE, AST, and, for agencies under the jurisdiction of the Governor, the Chief Inspector General. In addition, the records, and portions thereof, may be released to a local government, another state agency, or a federal agency for IT security purposes or in furtherance of the state agency’s official duties.¹⁹

Citizens Property Insurance Corporation

Citizens Property Insurance Corporation (Citizens) is a state-created, not-for-profit, tax-exempt governmental entity whose public purpose is to provide property insurance coverage to those unable to find affordable coverage in the voluntary admitted²⁰ market. It is not a private insurance company.²¹

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 public record requirements.²² Public disclosure of this information presents a significant security risk and would reveal weaknesses within Citizens’ computer networks, raising the potential for exploitation.

Section 282.318, F.S., exempts from public record requirements data and information from technology systems owned, contracted, or maintained by a state agency. However, s. 282.318(2), F.S., defines “state agency” as having the same meaning as provided in s. 282.0041, F.S. State agency is defined in s. 282.0041(23), F.S., as meaning:

[A]ny 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.

Because Citizens is not created within the executive branch, it is not covered by the definition.

Therefore, Citizens is vulnerable to the disclosure of 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.²³

Effect of the Bill

The bill creates public record and public meeting exemptions to protect data and records pertaining to the security of the Citizens information networks from disclosure. The bill provides that 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

¹⁸ Section 282.318(4)(i) and (5), F.S.

¹⁹ *Id.*

²⁰ Admitted market means insurance companies licensed to transact insurance in Florida.

²¹ Section 627.351(6)(a).1., F.S.

²² FLA. CONST. art. I, s. 24 (c); ch. 119, F.S.

²³ 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.

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.

The bill also creates 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.

The bill requires the confidential and exempt records related to the public meeting exemption to be available to the Auditor General, the Cybercrime Office of DLE, and the Office of Insurance Regulation. Such records and portions of meetings, recordings, and transcripts may also be available to a state or federal agency for security purposes or in furtherance of the agency's official duties.

The public record exemptions are retroactive and apply to records held by Citizens before, on, or after the effective date of the bill.

The bill provides a public necessity statement as required by the State Constitution, specifying that the public record and public meeting exemptions are necessary to ensure effective investigations of IT security breaches, to prevent identity theft and other crimes, and to prevent the disclosure of weaknesses in Citizens' data security.

The bill provides for repeal of the exemptions on October 2, 2023, unless reviewed and saved from repeal through reenactment by the Legislature.

B. SECTION DIRECTORY:

Section 1. creates s. 627.352, F.S., relating to security of data and information technology in Citizens Property Insurance Corporation.

Section 2. provides a public necessity statement.

Section 3. provides an effective date of upon becoming a law.

II. FISCAL ANALYSIS & ECONOMIC IMPACT STATEMENT

A. FISCAL IMPACT ON STATE GOVERNMENT:

1. Revenues:

The bill does not appear to impact state government revenues.

2. Expenditures:

See Fiscal Comments.

B. FISCAL IMPACT ON LOCAL GOVERNMENTS:

1. Revenues:

The bill does not appear to impact local government revenues.

2. Expenditures:

The bill does not appear to impact local government expenditures.

C. DIRECT ECONOMIC IMPACT ON PRIVATE SECTOR:

None.

D. FISCAL COMMENTS:

The bill may create a minimal fiscal impact on Citizens because staff responsible for complying with public record requests and public meeting requirements could require training related to the creation of the public record and public meeting exemptions. In addition, Citizens could incur costs associated with redacting the exempt information prior to releasing a record. The costs, however, would be absorbed, as they are part of the day-to-day responsibilities of Citizens.

III. COMMENTS

A. CONSTITUTIONAL ISSUES:

1. Applicability of Municipality/County Mandates Provision:

Not applicable. The bill does not appear to affect county or municipal governments.

2. Other:

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 newly created or expanded public record or public meeting exemption. The bill creates public record and public meeting exemptions; thus, it requires a two-thirds vote for final passage.

Public Necessity Statement

Article I, s. 24(c) of the State Constitution requires a public necessity statement for a newly created or expanded public record or public meeting exemption. The bill creates public record and public meeting exemptions; thus, it includes a public necessity statement.

Breadth of Exemption

Article I, s. 24(c) of the State Constitution requires a newly created public record or public meeting exemption to be no broader than necessary to accomplish the stated purpose of the law. The bill creates public record exemptions for records held by Citizens that identify detection, investigation, or response practices for suspected or confirmed IT security incidents in addition to a public meeting exemption for portions of public meetings that would reveal such data and information. As such, the exemptions do not appear to be in conflict with the constitutional requirement that the exemptions be no broader than necessary to accomplish the stated purpose.

B. RULE-MAKING AUTHORITY:

The bill does not appear to create a need for rulemaking or rulemaking authority.

C. DRAFTING ISSUES OR OTHER COMMENTS:

None.

IV. AMENDMENTS/ COMMITTEE SUBSTITUTE CHANGES

On January 17, 2018, the Oversight, Transparency & Administration Subcommittee adopted an amendment and reported the bill favorably as a committee substitute. The amendment:

- Expanded the bill's relating to clause to include public meetings;
- Changed the effective date of the bill to "upon becoming a law;" and
- Changed the automatic repeal date of the bill from October 2, 2022, to October 2, 2023.

On February 13, 2018, the Government Accountability Committee adopted an amendment and reported the bill favorably as a committee substitute. The amendment removed a drafting error that provided retroactive application of the public meeting exemption.

This analysis is drafted to the committee substitute as approved by the Government Accountability Committee.