HOUSE OF REPRESENTATIVES STAFF ANALYSIS

BILL #: CS/CS/HB 1037 Public Records/State Agency Information Technology Security Programs
SPONSOR(S): State Affairs Committee; Government Operations Subcommittee; Artiles
TIED BILLS: CS/CS/CS/HB 1033 **IDEN./SIM. BILLS:** CS/SB 624

REFERENCE	ACTION	ANALYST	STAFF DIRECTOR or BUDGET/POLICY CHIEF
1) Government Operations Subcommittee	13 Y, 0 N, As CS	Toliver	Williamson
2) State Affairs Committee	15 Y, 0 N, As CS	Toliver	Camechis

SUMMARY ANALYSIS

The Information Technology (IT) Security Act requires the Agency for State Technology (AST) and state agency heads to meet certain requirements relating to IT security. Currently, the IT Security Act provides public record exemptions for state agency comprehensive risk assessments, certain internal policies and procedures of state agencies, and the results of internal audits and evaluations.

The bill creates additional public record exemptions within the IT Security Act. It provides that records held by a state agency that identify detection, investigation, or response practices for suspected or confirmed IT security incidents are confidential and exempt from public records requirements. In addition, the bill provides that 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 are confidential and exempt. 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.

The bill authorizes the release of the confidential and exempt records, and portions thereof, to certain entities.

The bill provides for retroactive application of the public record exemptions. It also provides that the exemptions repeal on October 2, 2021, unless reviewed and saved from repeal by the Legislature. Finally the bill provides a statement of public necessity as required by the Florida Constitution.

Article I, s. 24(c) of the Florida 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 exemptions for certain records relating to IT security; thus, it requires a two-thirds vote for final passage.

FULL ANALYSIS

I. SUBSTANTIVE ANALYSIS

A. EFFECT OF PROPOSED CHANGES:

Background

Public Records

The Florida Constitution guarantees every person the right to inspect or copy any public record made or received in connection with the official business of the legislative, executive, or judicial branches of government.[1] The Legislature, however, may provide by general law for the exemption of records from the constitutional requirement.[2] The general law must state with specificity the public necessity justifying the exemption and must be no broader than necessary to accomplish the stated purpose of the law.[3] A bill enacting an exemption must pass by a two-thirds vote of the members present and voting.[4]

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. Furthermore, the Open Government Sunset Review Act[5] provides that a public record 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 effectively and efficiently administer a government program, which administration would be significantly impaired without the exemption;
- Protect personal identifying information that, if released, would be defamatory or would jeopardize an individual's safety; or
- Protect trade or business secrets.[6]

The Open Government Sunset Review Act requires the automatic repeal of a newly created exemption on October 2 of the fifth year after creation or substantial amendment, unless the Legislature reenacts the exemption.[7]

Information Technology Security Act

The Information Technology (IT) Security Act[8] requires the Agency for State Technology (AST)[9] and the heads of state agencies[10] to meet certain requirements to enhance the IT[11] security of state agencies. Specifically, the IT Security Act provides that the AST is responsible for establishing standards and processes consistent with generally accepted best practices for IT security and adopting rules that safeguard an agency's data, information, and IT resources to ensure availability, confidentiality, and integrity.[12] In addition, the AST must:

- Develop, and annually update, a statewide IT security strategic plan;

[1] FLA. CONST., art. I, s. 24(a).
[2] FLA. CONST., art. I, s. 24(c).
[3] *Id.*
[4] *Id.*
[5] Section 119.15, F.S.
[6] Section 119.15(6)(b), F.S.
[7] Section 119.15(3), F.S.
[8] Section 282.318, F.S.
[9] The AST is administratively housed within the Department of Management Services, and is tasked with developing IT policy for management of the state's IT resources. *See* ss. 20.61 and 282.0051, F.S.
[10] The term "state agency" is defined to mean 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. Section 282.0041(23), F.S.
[11] The term "information technology" is defined to mean 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. Section 282.0041(11), F.S.
[12] Section 282.318(3), F.S.

- Develop and publish an IT security framework for state agencies;
- Collaborate with the Cybercrime Office within the Florida Department of Law Enforcement (FDLE) in providing training for state agency information security managers; and
- Annually review the strategic and operational IT security plans of executive branch agencies.[13]

The IT Security Act requires the head of each state agency[14] to designate an information security manager to administer the IT security program of the state agency.[15] In addition, the head of each state agency must annually submit to the AST the state agency's strategic and operational IT security plans; conduct, and update every three years, a comprehensive risk assessment to determine the security threats to the data, information, and IT resources of the state agency; develop, and periodically update, written internal policies and procedures; and ensure that periodic internal audits and evaluations of the agency's IT security program for the data, information, and IT resources are conducted.[16]

Current Public Record Exemptions under the IT Security Act

Currently, the IT Security Act provides that the following state agency information is confidential and exempt[17] from s. 119.07(1), F.S.:

- Comprehensive risk assessments;[18]
- Internal policies and procedures that, if disclosed, could facilitate the unauthorized modification, disclosure, or destruction of data or information technology resources;[19]
- The results of internal audits and evaluations.[20]

The confidential and exempt information must be disclosed to the Auditor General, the Cybercrime Office within FDLE, the AST, and, for agencies under the jurisdiction of the Governor, the Chief Inspector General.[21]

CS/CS/CS/HB 1033 (2016)

CS/CS/CS/HB 1033 makes several changes to the IT Security Act. In part, the bill requires:

- The AST to establish standards and processes consistent with best practices for both IT security and cybersecurity.
- The AST to develop and publish guidelines and processes for an IT security framework for use by state agencies.
- Each state agency head to implement risk assessment remediation plans recommended by the AST.
- Each state agency head to report an IT security incident or breach to the Cybercrime Office within FDLE.

Effect of the Bill

[13] Section 282.318(3), F.S.

[14] The term "state agency" is defined to mean 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. Section 282.0041(23), F.S. For purposes of the IT Security Act, the Department of Legal Affairs, the Department of Agriculture and Consumer Services, or the Department of Financial Services. Section 282.318(2), F.S.

[15] Section 282.318(4)(a), F.S.

[16] Section 282.318(4), F.S.

[17] 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).

[18] Section 282.318(4)(c), F.S.

[19] Section 282.318(4)(d), F.S.

[20] Section 282.318(4)(f), F.S.

[21] Section 282.318(4)(c), F.S.; s. 282.318(4)(f), F.S.

The bill, which is linked to the passage of CS/CS/CS/HB 1033, creates additional public record exemptions within the IT Security Act. The bill 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 from public records requirements. In addition, the bill provides that 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, which are held by a state agency, are confidential and exempt from public records requirements. 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:
  - 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.

For purposes of the public record exemptions, the term "external audit" means an audit that is conducted by an entity other than the state agency that is the subject of the audit.

The confidential and exempt records, and portions thereof, must be made available to the Auditor General, the AST, the Cybercrime Office within FDLE, and, for those agencies under the jurisdiction of the Governor, the Chief Inspector General. The bill further provides that the confidential and exempt 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.

The bill provides for retroactive application of the public record exemptions.[22] It also provides for repeal of the exemptions on October 2, 2021, unless reviewed and saved from repeal through reenactment by the Legislature. Finally, the bill provides a public necessity statement as required by the Florida Constitution.

B. SECTION DIRECTORY:

Section 1 amends s. 282.318, F.S., relating to security of data and IT.

Section 2 provides a public necessity statement.

Section 3 provides an effective date that is contingent upon the passage of CS/CS/CS/HB 1033 or similar legislation.

II. FISCAL ANALYSIS & ECONOMIC IMPACT STATEMENT

A. FISCAL IMPACT ON STATE GOVERNMENT:

1. Revenues:

   None.

2. Expenditures:

   The bill could have a minimal fiscal impact on state agencies because staff responsible for complying with public records requests may require training related to creation of the public record

[22] The Supreme Court of Florida ruled that a public record exemption is not to be applied retroactively unless the legislation clearly expresses intent that such exemption is to be applied as such. Access to public records is a substantive right. Thus, a statute affecting that right is presumptively prospective and there must be a clear legislative intent for the statute to apply retroactively. *See Memorial Hospital-West Volusia, Inc. v. News-Journal Corporation*, 784 So. 2d 438, 441 (Fla. 2001).

exemptions. In addition, agencies could incur costs associated with redacting the confidential and exempt records prior to release. The costs, however, would be absorbed, as they are part of the day-to-day responsibilities of state agencies.

B. FISCAL IMPACT ON LOCAL GOVERNMENTS:

1. Revenues:

None.

2. Expenditures:

None.

C. DIRECT ECONOMIC IMPACT ON PRIVATE SECTOR:

None.

D. FISCAL COMMENTS:

None.

III. COMMENTS

A. CONSTITUTIONAL ISSUES:

1. Applicability of Municipality/County Mandates Provision:

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

2. Other:

Vote Requirement
Article I, section 24(c) of the Florida 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 exemptions; therefore, it requires a two-thirds vote for final passage.

Public Necessity Statement
Article I, section 24(c) of the Florida Constitution requires a public necessity statement for a newly created or expanded public record or public meeting exemption. The bill creates public record exemptions; therefore, it includes a public necessity statement.

Breadth of Exemption
Article I, section 24(c) of the Florida 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 certain state agency records, and portions thereof, related to IT security. The release of such records could result in the identification of vulnerabilities or gaps in a state agency's IT security system or process and thereby increase the risk of an IT security incident or breach. Thus, the bill does not appear to be in conflict with the constitutional requirement that an exemption be no broader than necessary to accomplish its purpose.

B. RULE-MAKING AUTHORITY:

None.

C. DRAFTING ISSUES OR OTHER COMMENTS:

None.

IV. AMENDMENTS/ COMMITTEE SUBSTITUTE CHANGES

On January 26, 2016, the Government Operations Subcommittee adopted two amendments and reported the bill favorably as a committee substitute. The amendments corrected drafting issues and made conforming changes.

On February 25, 2016, the State Affairs Committee adopted a proposed committee substitute and reported the bill favorably as a committee substitute. The proposed committee substitute:

- Removed the public record exemption for third party risk assessments because the provision requiring such risk assessments was removed from CS/CS/CS/HB 1033, which this bill is linked to for final passage;
- Created a public record exemption for records held by a state agency that identify detection, investigation, or response practices for suspected or confirmed IT security incidents;
- Created a public record exemption for 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;
- Provided that the 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;
- Required that the confidential and exempt records be made available to the Auditor General, the AST, the Cybercrime Office within FDLE, and, for those agencies under the jurisdiction of the Governor, the Chief Inspector General;
- Authorized release of the confidential and exempt records 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; and
- Provided for retroactive application of the public record exemptions.

This analysis is drafted to the committee substitute as approved by the State Affairs Committee