

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 624

INTRODUCER: Senator Hays

SUBJECT: Public Records/State Agency Information Technology Security Programs

DATE: November 30, 2015 REVISED: _____

	ANALYST	STAFF DIRECTOR	REFERENCE	ACTION
1.	Kim	McVaney	GO	Pre-meeting
2.			RC	

I. Summary:

SB 624 provides a public records exemption that information relating to information technology security incidents or breaches. Such information will be confidential and exempt if the information could facilitate unauthorized access or destruction of data or information technology resources.

The bill also provides that external audits and evaluations of a state agency's information technology security systems are confidential and exempt from public disclosure.

The bill will go into effect upon becoming law.

This is a new public records exemption, so a two-thirds vote by each chamber will be necessary for passage.

II. Present Situation:

Public Records Law

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

¹ FLA. CONST., art. I, s. 24(a).

² FLA. CONST., art. I, s. 24(a).

In addition to the Florida Constitution, the Florida Statutes provides that the public may access legislative and executive branch records.³ Chapter 119, F.S., constitutes the main body of public records laws, and is known as the Public Records Act.⁴ The Public Records Act states that

it 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.⁵

According to the Public Records Act, a public record includes virtually any document or recording, regardless of its physical form or how it may be transmitted.⁶ The Florida Supreme Court has interpreted public records as being “any material prepared in connection with official agency business which is intended to perpetuate, communicate or formalize knowledge of some type.”⁷ A violation of the Public Records Act may result in civil or criminal liability.⁸

The Legislature may create an exemption to public records requirements.⁹ An exemption must pass by a two-thirds vote of the House and the Senate.¹⁰ In addition, an exemption must explicitly lay out the public necessity justifying the exemption, and the exemption must be no broader than necessary to accomplish the stated purpose of the exemption.¹¹ A statutory exemption which does not meet these criteria may be unconstitutional and may not be judicially saved.¹²

When creating a public records exemption, the Legislature may provide that a record is ‘confidential and exempt’ or ‘exempt.’¹³ Records designated as ‘confidential and exempt’ may

³ The Public Records Act does not apply to legislative or judicial records. *Locke v. Hawkes*, 595 So. 2d 32 (Fla. 1992). Also see *Times Pub. Co. v. Ake*, 660 So. 2d 255 (Fla. 1995). The Legislature’s records are public pursuant to s. 11.0431, F.S. Public records exemptions for the Legislatures are primarily located in s. 11.0431(2)-(3), F.S.

⁴ Public records laws are found throughout the Florida Statutes.

⁵ Section 119.01(1), F.S.

⁶ Section 119.011(12), F.S., defines “public record” to mean “all documents, papers, letters, maps, books, tapes, photographs, films, sound recordings, data processing software, or other material, regardless of the physical form, characteristics, or means of transmission, made or received pursuant to law or ordinance or in connection with the transaction of official business by any agency.” Section 119.011(2), F.S., defines “agency” to mean 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.”

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

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 FLA. CONST., art. I, s. 24(c).

¹¹ FLA. CONST., art. I, s. 24(c).

¹² *Halifax Hosp. Medical Center v. New-Journal Corp.*, 724 So.2d 567 (Fla. 1999). In *Halifax Hospital*, the Florida Supreme Court found that a public meetings exemption was unconstitutional because the statement of public necessity did not define important terms and did not justify the breadth of the exemption. *Id.* at 570. The Florida Supreme Court also declined to narrow the exemption in order to save it. *Id.* In *Baker County Press, Inc. v. Baker County Medical Services, Inc.*, 870 So. 2d 189 (Fla. 1st DCA 2004), the court found that the intent of a statute was to create a public records exemption. The *Baker County Press* court found that since the law did not contain a public necessity statement, it was unconstitutional. *Id.* at 196.

¹³ If the Legislature designates a record as confidential, such record may not be released to anyone other than the persons or entities specifically designated in the statutory exemption. *WFTV, Inc. v. The School Board of Seminole*, 874 So. 2d 48 (Fla. 5th DCA 2004).

be released by the records custodian only under the circumstances defined by the Legislature. Records designated as ‘exempt’ may be released at the discretion of the records custodian.¹⁴

Open Government Sunset Review Act

In addition to the constitutional requirements relating to the enactment of a public records exemption, the Legislature may subject the new or broadened exemption to the Open Government Sunset Review Act (OGSR).

The OGSR prescribes a legislative review process for newly created or substantially amended public records.¹⁵ The OGSR provides that an exemption automatically repeals 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.¹⁶ In practice, many exemptions are continued by repealing the sunset date rather than reenacting the exemption.

If the Legislature expands an exemption, then a public necessity statement and a two-thirds vote for passage are required.¹⁷ If the exemption is reenacted 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 sunset, the previously exempt records will remain exempt unless otherwise provided for by law.¹⁸

Agency for State Technology

The Agency for State Technology (AST) is responsible for establishing standard for information technology security for state agencies.¹⁹ AST is responsible for assisting agencies in performing the following functions:

- Completing risk assessments and information technology security audits, which must be submitted to AST;²⁰
- Establishing procedures for accessing information to ensure confidentiality and integrity of the data;²¹
- Responding to and recovering from security breaches;²²

¹⁴ A record classified as exempt from public disclosure may be disclosed under certain circumstances. *Williams v. City of Minneola*, 575 So. 2d 687 (Fla. 5th DCA 1991).

¹⁵ Section 119.15, F.S. According to s. 119.15(4)(b), F.S., a substantially amended exemption is one that is expanded to include more information or to include meetings. The OGSR does not apply to an exemption that is required by federal law or that applies solely to the Legislature or the State Court System pursuant to s. 119.15(2), F.S. The OGSR process is currently being followed, however, the Legislature is not required to continue to do so. The Florida Supreme Court has found that one legislature cannot bind a future legislature. *Scott v. Williams*, 107 So. 3d 379 (Fla. 2013).

¹⁶ Section 119.15(3), F.S.

¹⁷ FLA. CONST., art. I, s. 24(c).

¹⁸ Section 119.15(7), F.S.

¹⁹ Section 282.318(3), F.S.

²⁰ Section 282.381(3)(b)3., F.S.

²¹ Section 282.381(3)(b)5., F.S.

²² Section 282.381(3)(b)7. and 8., F.S.

In addition, each state agency head is required to perform the following functions:²³

- Designate an information security manager;
- Annually submit to AST the agency's information technology security plan consistent with AST rules and guidelines;
- Conduct a comprehensive risk assessment every three years consistent with AST risk assessment methodology;
- Develop protocols for reporting information technology security incidents and breaches to the Cybercrime Office of the Department of Law Enforcement (FDLE) and AST;
- Implement safeguards established by AST to address risk to the agency's information and technology;
- Ensure internal audits and evaluations of the agency's information technology are conducted;
- Include information technology security requirements consistent with AST and Department of Management Services protocols in solicitations for procurements;
- Train employees about information technology security risks and protocols; and
- Develop a process for detecting, responding to and reporting information security breaches. State agencies must report each security incidents and breaches to AST, as well as the Department of Legal Affairs, individuals whose personal information was involved, and credit reporting agencies under certain circumstances.²⁴

The following information is confidential and exempt from public records laws:

- Comprehensive risk assessments pursuant to s. 282.318(4)(c), F.S.;
- Internal policy and procedures that could facilitate the unauthorized modification, disclosure or destruction of data or information technology resources, pursuant s. 282.318(4)(d), F.S.; and
- Internal audit reports and evaluations of an agency's information technology security resources, pursuant to s. 282.318(4)(f), F.S.

These documents must be released to the Auditor General, the Cybercrime Office of FDLE, AST, and the Chief Inspector General.

III. Effect of Proposed Changes:

Section 1 makes confidential and exempt those records held by a state agency related to the detection, investigation or response to a security incident. This includes records relating to suspected or confirmed security incidents or breaches. The information is confidential and exempt only if the disclosure of such records could facilitate:

- Unauthorized access to data or information technology resources; or
- Unauthorized modification, disclosure or destruction of data or information technology resources.

State agencies are permitted to release the confidential and exempt information to AST and the Cybercrimes Office of the FDLE. State agencies under the jurisdiction of the Governor are also permitted to release the confidential and exempt information to the Chief Inspector General. The bill provides for retroactive application; thus information held by a state agency before this

²³ Section 282.318(4), F.S.

²⁴ Section 282.318(4)(i), F.S. and s. 501.171, F.S.

exemption becomes law will become confidential and exempt. This exemption will also be subject to review and repeal on October 2, 2021, pursuant to the OGSR.

The bill provides a public records exemption for external audits and evaluations of a state agency's information technology security program for data, information, and information technology resources. This information will be confidential and exempt from public disclosure. A state agency is authorized to share the information with AST and the Cybercrimes Office of the FDLE. State agencies which are under the jurisdiction of the Governor, are also permitted to release the external audits and evaluations to the Chief Inspector General. The bill allows external audits and evaluations to be made available to other state agencies for information technology purposes. The bill appears to limit access to the external audits and evaluations to agencies for a limited purpose, thereby limiting when such information may be released.

The bill provides for retroactive application, thus information held by a state agency before this exemption becomes law would become confidential and exempt. This exemption will also be subject to review and repeal on October 2, 2021, pursuant to the OGSR.

Section 2 provides the public necessity statement required by the Florida Constitution. The public necessity for the exemption for external audits includes several parts.

Paragraph (1)(a) states that releasing information related to security incidents and breaches could impede and impair investigations and that releasing such information before it is complete could jeopardize the investigation.

Paragraph (1)(b) states that investigations of security incidents is likely to include sensitive personal information (such as social security numbers, financial or health information) and such information could be used for purposes of identity theft if it were made public. In addition, health information has traditionally been considered private between an individual and a health care provider, which is considered confidential in both public and private sectors.

Paragraph (1)(c) provides that the release of a computer forensic report or other information upon the conclusion of an investigation could reveal security weaknesses that could compromise the agency in the future, as well compromise other agencies.

Paragraph(1)(d) provides that information held by an agency relating to a security breach or incident may contain proprietary information or trade secret information about the security system at issue. The public necessity statement goes on to state that the release of such information could cause financial loss and give a business's competitors an unfair advantage.

Paragraph (1)(e) states that disclosure of "such information" could compromise the integrity of state agency data and information technology resources and impair the administration of government programs. This paragraph also states that the exemption should be retroactive because it is remedial in nature.

Subsection 2 contains the public necessity statement for the results of external audits and evaluations of a state agency's information technology security system. The bill provides that state agencies may find an audit by an independent entity of its information technology system to

be valuable. An independent audit could identify vulnerabilities in systems and make recommendations for remedies. The disclosure of those external audits would compromise the integrity of agency information technology resources. The bill goes on to state that the exemption is remedial in nature, and should be given retroactive application.

IV. Constitutional Issues:

A. Municipality/County Mandates Restrictions:

The mandate restrictions do not apply because the bill does not require counties and municipalities to spend funds, reduce counties' or municipalities' ability to raise revenue, or reduce the percentage of a state tax shares with counties and municipalities.

B. Public Records/Open Meetings Issues:

The public necessity statement appears to contain terms which are not sufficiently defined. The statement contains legislative findings which do not appear to be relevant to the exemption. As previously noted, an exemption must explicitly lay out the public necessity justifying the exemption, and the exemption must be no broader than necessary to accomplish the stated purpose of the exemption.²⁵ A statutory exemption which does not meet these criteria may be unconstitutional and may not be judicially saved.

C. Trust Funds Restrictions:

None.

V. Fiscal Impact Statement:

A. Tax/Fee Issues:

None.

B. Private Sector Impact:

There is no known private sector impact from this bill. However, the public necessity statement suggests that this bill will help private sector businesses.²⁶

C. Government Sector Impact:

Unknown. Presumably, the redactions will create additional work for records custodians, however, this most likely will be absorbed by existing agency resources.²⁷

²⁵ FLA. CONST., art. I, s. 24(c).

²⁶ 2015 Agency Legislative Bill analysis by the State Agency by AST dated November 3, 2015. FDLE and the Auditor General did not comment on this issue in the bill analyses.

²⁷ The bill analyses provided by AST, FDLE and the Auditor General indicate that this bill will not impact their agencies.

VI. Technical Deficiencies:

Public records exemptions usually state that records are held by one or more agencies. The bill does not state which agency is the holder of the relevant information.

Section 2, paragraph (1)(a): Nothing in the substantive portion of the bill allows a completed investigation to be made public. The public necessity statement, however, argues that ongoing security breach investigations should be exempt, but then does not follow through with why an investigation should not be made public once it is completed. This gives the impression that security breach information should be public after an investigation is completed.²⁸

Section 2, paragraph (1)(b): Some of personal information, such as social security²⁹ numbers, are already protected by general public records exemptions.

Section 2, paragraph (1)(c): This portion of the public necessity statement addresses why information should be remain confidential and exempt after an investigation is complete. This statement picks up the justification of the exemption where paragraph (1)(a) ended. The substantive portion of the bill does not make any reference to complete or incomplete investigations, so it is not clear why the public necessity statement makes such a distinction. In addition, it is not clear why paragraph (1)(a) and (1)(c) are separated by (1)(b).

Section 2, paragraph (1)(d): This portion of the public necessity statement provides that information which relates to the detection or investigation of security breaches should be confidential and exempt because such information is proprietary business information or trade secret. There is no single exemption for proprietary business information, so if AST wishes to pursue one for their vendors, a separate bill may be required.

There are several exemptions for computer related trade secrets in current law. Data, programs or supporting documentation that are trade secret held by any agency are confidential and exempt pursuant to s. 815.04(3), F.S., and s. 815.045, F.S., has been interpreted by the First District Court of Appeals to be a general trade secret exemption for all agencies.³⁰ In addition, data processing software is already exempt pursuant to s. 119.071(1)(f), F.S. Since there are protections for trade secret computer-related information, the public necessity statement in this bill which supports the AST exemption on the grounds of protecting trade secrets appears to be unnecessary.

There appears to be a spelling error on line 106. The word “conformed” should probably be confirmed.

Section 2 subsection (2): This language implies that an external audit is an audit performed by an independent entity, however, it is not clear from the statute or the bill if an independent entity includes another agency (such as AST) or a contractor hired by an agency to audit that agency’s

²⁸ Public records exemptions for some investigations expire when the investigations are complete. For example, s. 119.071(2)(c), F.S., provides that criminal investigations are exempt only as long as they are active, and s. 119.0713(2), F.S., provides that internal audit reports and inspector general reports are confidential exempt until they are final.

²⁹ Section 119.071(5), F.S.

³⁰ *SEPRO Corp. v. Florida Dept. of Environmental Protection*, 839 So. 2d 781 (Fla. 1st DCA 2003).

information technology systems. This distinction is important in that it is not clear that AST has any statutory authority to perform an audit on another state agency. It is also unclear to what extent an audit by an independent auditor who is a contracted agent of an agency would be considered 'external' and therefore, not covered by the currently existing public records exemption for internal audits as provided in s. 282.318(4)(f), F.S. A risk assessment performed by an agency is currently confidential and exempt under s. 282.318(c), F.S., and it is not clear why an external audit would not qualify as risk assessment.

VII. Related Issues:

None.

VIII. Statutes Affected:

This bill substantially amends section 282.318 of the Florida Statutes.

IX. Additional Information:

A. Committee Substitute – Statement of Changes:

(Summarizing differences between the Committee Substitute and the prior version of the bill.)

None.

B. Amendments:

None.