HOUSE OF REPRESENTATIVES STAFF ANALYSIS

BILL #: CS/HB 1287 Pub. Rec./Information Held by a Utility Owned or Operated by a Unit of Local Government
SPONSOR(S): Tourism, Infrastructure & Energy Subcommittee, Botana and Yarborough
TIED BILLS: **IDEN./SIM. BILLS:** SB 1740

REFERENCE	ACTION	ANALYST	STAFF DIRECTOR or BUDGET/POLICY CHIEF
1) Tourism, Infrastructure & Energy Subcommittee	16 Y, 0 N, As CS	Neuffer	Keating
2) Government Operations Subcommittee			
3) Commerce Committee			

SUMMARY ANALYSIS

Under current law, information related to security of the technology, processes, or practices designed to protect existing or proposed information technology systems, or industrial control systems held by a utility owned or operated by a unit of local government, is exempt from disclosure as public records.

The bill amends the public record exemption for information held by a utility owned or operated by a unit of local government to include:

- Information related to threat detection, defense, deterrence, or response plans and action for information technology (IT) and operational technology (OT) systems;
- Information related to insurance or other risk mitigation products or coverages for the protection of the IT and OT systems and data; and
- Critical energy infrastructure information, whether created or received by the utility.

Critical energy infrastructure information is defined as specific engineering, vulnerability, or detailed design information about proposed or existing critical infrastructure which:

- Includes details about the production, generation, transportation, transmission, or distribution of energy;
- Could be useful in planning an attack on critical infrastructure; and
- Provides more than a general location of critical energy infrastructure.

Critical infrastructure is defined as existing or proposed systems and assets, whether physical or virtual, the incapacity or destruction of which would negatively affect security, economic security, public health, or public safety.

The bill provides that these public record exemptions are subject to repeal under the Open Government Sunset Review Act unless the Legislature reviews and reenacts the exemptions by October 2, 2027.

The bill provides a public necessity statement for each exemption as required by the Florida Constitution.

The bill does not appear to impact state or local government revenues or state government expenditures. The bill may impact local government expenditures.

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 a public record exemption; thus, it requires a two-thirds vote for final passage.

The bill has an effective date of July 1, 2022.

FULL ANALYSIS

I. SUBSTANTIVE ANALYSIS

A. EFFECT OF PROPOSED CHANGES:

Present Situation

Public Records

Article I, section 24(a) of the Florida 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. The Legislature, however, may provide by general law for the exemption of records from the requirements of article I, section 24(a) of the Florida Constitution.[1] The general law must state with specificity the public necessity justifying the exemption[2] and must be no broader than necessary to accomplish its purpose.[3]

Public policy regarding access to government records is addressed further in s. 119.07(1)(a), F.S., which guarantees every person a right to inspect and copy any state, county, or municipal record, unless the record is exempt. Furthermore, the Open Government Sunset Review Act[4] provides that a public record or public meeting exemption may be created or maintained only if it serves an identifiable public purpose and may be no broader than necessary to meet one of the following purposes:

- Allow the state or its political subdivisions to effectively and significantly administer a governmental program, which administration would be significantly impaired without the exemption.
- 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.[5]

The Open Government Sunset Review Act requires the automatic repeal of a newly created public record exemption on October 2nd of the fifth year after creation or substantial amendment of the exemption, unless the Legislature reenacts the exemption.[6]

Cybersecurity

Operational technology (OT) is the hardware and software which monitors and controls devices, processes, and infrastructure.[7] Informational technology (IT) combines two or more technologies to manage data and applications.[8] IT is used to monitor, manage, and secure core functions and data which are stored in the data center or cloud of an organization. OT, on the other hand, is used for connecting, monitoring, managing and securing an organization's industrial operations.[9] OT devices are distinct from most IT devices as they generally contain specialized software. Within the OT sector are industrial control systems (ICS) which function to monitor and control the actual operation of physical equipment and plant process automation and production.[10] Essentially, ICS are a combination of OT and IT technologies.

---

[1] Art. 1, s. 24(a), Fla. Const.
[2] This portion of a public record exemption is commonly referred to as a "public necessity statement."
[3] Art. 1, s. 24(c). Fla. Const.
[4] S. 119.15, F.S.
[5] S. 119.15(6)(b), F.S.
[6] S. 119.15(3), F.S.
[7] Cisco, *How Do OT and IT Differ?*, https://www.cisco.com/c/en/us/solutions/internet-of-things/what-is-ot-vs-it.html (last visited January 27, 2022).
[8] https://www.cisco.com/c/en/us/solutions/internet-of-things/what-is-ot-vs-it.html
[9] *Id.*
[10] David Meltzer & Jeff Lund, Industrial Cyber Security for Dummies 5 (John Wiley & Sons, Inc., Belden/Tripwire Special ed. 2017).

ICS are vital across a vast number of industries to ensure that processes and systems run effectively, making them a target for cyber threats in recent years.[11] On May 29, 2019, Riviera Beach was the target of a ransomware attack which paralyzed their computer systems, including the water utility.[12] The systems controlling both the pumping stations and water quality testing were compromised in the ransomware attack. The city council approved their insurance company to pay approximately $600,000 to the attackers in order to regain control of the systems.[13] The city paid an additional $25,000 to the insurance company for the cybersecurity policy deductible.[14] Due to the increased numbers of ransomware attacks in recent years, and the resulting claims to insurance companies, premiums are expected to increase by 25 percent to 40 percent across many industries.[15] Ransomware operators are taking advantage of the increased insurance coverage, viewing insured companies as key targets for cyberattacks.[16]

Information related to the procedures and practices a utility which is owned or operated by a unit of local government is exempt from the requirements of Florida's public records law.[17] These procedures and practices must be designed to protect a utility's network, computers, programs, and data from attack, damage, or unauthorized access which, if disclosed, would negatively impact the relevant data or information. Additionally, utility owned or operated by a unit of local government is exempt from disclosing information related to the security of their data processes, existing or proposed, and IT systems.[18] These exemptions are meant to protect information which, if disclosed, would cause the alteration, adverse impact, disclosure, or destruction of the exempt information or operation and systems of the utility.[19]

In 2011, the federal government enacted the Critical Infrastructures Protection Act (act) to protect the increasingly relied upon critical physical and information infrastructures across a vast number of industries.[20] These include telecommunications, energy, financial services, water, and transportation sectors.[21] The act aimed to create a comprehensive and effective program to ensure the continuity of essential functions.[22] Critical infrastructure is defined in the act as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[23] Recently, the federal government has launched an ICS Initiative in an attempt to encourage electric utilities and natural gas pipelines to deploy control system cybersecurity technologies to bolster the security and resilience of their facilities.[24] The initiative will be expanded to include the water sector as well.[25]

Effect of the Bill

---

[11] *See* https://www.cisa.gov/uscert/ics/content/cyber-threat-source-descriptions for more in-depth discussion about the threats targeting ICS.
[12] *Id.*
[13] *Id.*
[14] *Id.*
[15] Laura Sanicola, *After Colonial Attack, Energy Companies Rush to Secure Cyber Insurance*, Reuters, (May 28, 2021) https://www.reuters.com/technology/after-colonial-attack-energy-companies-rush-secure-cyber-insurance-2021-05-28/ (last visited January 27, 2022).
[16] *See* Matthew Delman, *Cyber Insurance May Be Making Ransomware Worse, Here's Why*, Morphisec (July 1, 2021), https://blog.morphisec.com/cyber-insurance-may-be-making-ransomware-worse-heres-why (last visited January 27, 2022) (explaining that ransomware groups target insured companies because insurers are more likely to pay the ransom).
[17] S. 119.0713(5)(a)(1), F.S.
[18] S. 119.0713(5)(a)(2), F.S.
[19] S. 119.0713(5)(a)(1) and (a)(2), F.S.
[20] *See* 42 U.S.C. § 5195c.
[21] 42 U.S.C. § 5195c(b)(3).
[22] 42 U.S.C. § 5195c(c)(3).
[23] 42 U.S.C. § 5195c(e).
[24] The White House, *Fact Sheet: Ongoing Public U.S. Efforts to Counter Ransomware* (October 13, 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/13/fact-sheet-ongoing-public-u-s-efforts-to-counter-ransomware/ (last visited January 27, 2022).
[25] *Id.*

The bill amends the public record exemption for certain information held by a utility owned or operated by a unit of local government to include:

- Information related to threat detection, defense, deterrence, or response plans and action for information technology (IT) and operational technology (OT) systems, including, but not limited to, plans and actions made or taken in response to a ransomware or cyberattack direct towards IT or OT systems;
- Information related to insurance or other risk mitigation products or coverages for the protection of IT and OT systems and data, including, but not limited to, deductible or self-insurance amounts, coverage limits, and policy terms and conditions; and
- Critical energy infrastructure information, whether created or received by the utility.

Critical energy infrastructure information is defined in the bill as specific engineering, vulnerability, or detailed design information about proposed or existing critical infrastructure which:

- Includes details about the production, generation, transportation, transmission, or distribution of energy;
- Could be useful in planning an attack on critical infrastructure; and
- Provides more than a general location of critical energy infrastructure.

All of the elements above are required in order to qualify as critical energy infrastructure information.

Critical infrastructure is defined as existing or proposed systems and assets, whether physical or virtual, the incapacity or destruction of which would negatively affect security, economic security, public health, or public safety.

This exemption applies retroactively to records already held by an agency and prospectively to future records. This exemption is subject to the Open Government Sunset Review Act and stands repealed on October 2, 2027, unless reviewed and saved from repeal by the Legislature.

The bill provides a public necessity statement as required by art. 1, s. 24(c) of the Florida Constitution. The statement provides that:

- Critical energy infrastructure information held by a utility owned or operated by a local government, if released, could result in danger or harm to the citizens of the state.
- Such information generally consists of critical asset location, vulnerable electric grid transmission information, emerging technologies utilized to prevent cyber-attacks, and secure information shared between utilities in the state, and regional and federal entities.
- The compromise of critical energy infrastructure information could lead to interruptions in the delivery of essential services, as well as financial or physical harm to the citizens of the state.
- Utilities in Florida have experienced recent cyber-attacks which have blocked access to, and control of, utility systems.
- Public disclosure of insurance coverages provides information to potential attackers as to the monetary limits which may be sought from utilities.
- Vulnerabilities expose these utilities, which control water, electricity, wastewater, and natural gas throughout the state, to cyber-attacks and ransom demands.
- The public benefit which may be derived from the disclosure of such information is outweighed by the harm that may result from its release.

The bill has an effective date of July 1, 2022.

B. SECTION DIRECTORY:

Section 1 Amends s. 119.0713, F.S.; relating to local government agency exemptions from inspection or copying of public records.

Section 2 Provides statement of public necessity.

Section 3 Provides an effective date.

II. FISCAL ANALYSIS & ECONOMIC IMPACT STATEMENT

A. FISCAL IMPACT ON STATE GOVERNMENT:

1. Revenues:

None.

2. Expenditures:

None.

B. FISCAL IMPACT ON LOCAL GOVERNMENTS:

1. Revenues:

None.

2. Expenditures:

The bill may have an insignificant negative fiscal impact on various state agencies because state agency staff responsible for complying with public record requests may require training related to the newly created public record exemption. These costs, however, would be absorbed, as they are part of the day-to-day responsibilities of each state agency.

The bill may lower the risk of cyberattacks on local government utility infrastructure, in turn lowering costs to the local government and its utility customers associated with cyberattacks.

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 require counties or municipalities to spend funds or take action requiring the expenditure of funds; reduce the authority that counties or municipalities have to raise revenues in the aggregate; or reduce the percentage of state tax shared with counties or municipalities.

2. Other:

Vote Requirement
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 a public record exemption; thus, it requires a two-thirds vote for final passage.

Public Necessity Statement
Article I, s. 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 includes a public necessity statement for each newly created exemption in the bill.

Breadth of Exemption

Article I, s. 24(c) of the Florida Constitution requires a newly created or expanded public record or public meeting exemption to be no broader than necessary to accomplish the stated purpose of the law.

The bill provides a public record exemption for information related to threat detection, defense, deterrence, or response plans and actions for IT and OT systems of a utility owned or operated by a unit of local government. This information includes, but is not limited to, plans and action made or taken in response to a ransomware or cyberattack on or threat to IT or OT systems. Additionally, the bill provides a public record exemption for information related to insurance or other risk mitigating products or coverages. This information includes, but is not limited to, deductible or self-insurance amounts, coverage limits, and policy terms and conditions, for the protection of IT and OT systems and data of a utility owned or operated by a unit of local government.

The bill also provides a public record exemption for critical energy infrastructure information created or received by a utility owned or operated by a unit of local government.

B. RULE-MAKING AUTHORITY:

This bill does not require or authorize rulemaking.

C. DRAFTING ISSUES OR OTHER COMMENTS:

IV. AMENDMENTS/COMMITTEE SUBSTITUTE CHANGES

On February 3, 2022, the Tourism, Infrastructure & Energy Subcommittee adopted one amendment and reported the bill favorably as a committee substitute. The amendment:

- Clarifies that the elements provided in defining critical energy infrastructure information are conjunctive.
- Elaborates the statement of public necessity to conform with the amendment.

This analysis is drafted to the committee substitute as approved by the Tourism, Infrastructure & Energy Subcommittee.