Energy, Communications & Cybersecurity Subcommittee

Thursday, January 25, 2024
3:00 PM - 6:00 PM
Reed Hall (102 HOB)

Meeting Packet

Paul Renner
Speaker

Mike Giallombardo
Chair

The Florida House of Representatives

Commerce Committee

Energy, Communications & Cybersecurity Subcommittee

Paul Renner
Speaker

Mike Giallombardo
Chair

Meeting Agenda

Thursday, January 25, 2024
3:00 pm – 6:00 pm
Reed Hall (102 HOB)

I. Call to Order

II. Roll Call

III. Welcome and Opening Remarks

IV. Consideration of the following bill(s):
- HB 1555 Cybersecurity by Giallombardo
- HB 7047 OGSR/Utility Owned or Operated by a Unit of Local Government by Ethics, Elections & Open Government Subcommittee, Porras

V. Cybersecurity Update

VI. Closing Remarks

VII. Adjournment

HOUSE OF REPRESENTATIVES STAFF ANALYSIS

BILL #: HB 1555 Cybersecurity
SPONSOR(S): Giallombardo
TIED BILLS: **IDEN./SIM. BILLS:** SB 1662

REFERENCE	ACTION	ANALYST	STAFF DIRECTOR or BUDGET/POLICY CHIEF
1) Energy, Communications & Cybersecurity Subcommittee		Bauldree	Keating
2) State Administration & Technology Appropriations Subcommittee			
3) Commerce Committee			

SUMMARY ANALYSIS

Over the last decade, cybersecurity has rapidly become a growing concern. Cyberattacks are growing in frequency and severity. Currently, the Department of Management Services (DMS) oversees information technology (IT) governance and security for the executive branch of state government. The Florida Digital Service (FLDS) is housed within DMS and was established in 2020 to replace the Division of State Technology. Through FLDS, DMS implements duties and policies for IT and cybersecurity for state agencies.

The bill:

- Revises the duties of FLDS;
- Provides definitions;
- Provides that the state chief information officer (CIO), in consultation with the Secretary of DMS, must designate a state chief technology officer and specifies the position's responsibilities;
- Requires FLDS to ensure independent project oversight on all state agency IT projects that have a total project cost of $25 million or more (up from $10 million in current law);
- Provides that FLDS no longer must conduct annual assessments of state agencies to determine compliance with IT standards and guidelines developed and published by DMS;
- Requires each state agency to designate a chief information security officer to integrate the agency's technical and operational cybersecurity efforts with Cybersecurity Operations Center (CSOC);
- Requires state agencies to report all ransomware incidents, regardless of severity level, to the CSOC as soon as possible, but no later than 12 hours after a cybersecurity incident and no later than 6 hours after the discovery of a ransomware incident;
- Requires local governments to report any cybersecurity incident determined to be level 3, 4, or 5 to the CSOC rather than the Cybercrime Office and the sheriff who has jurisdiction over the local government;
- Requires CSOC to immediately notify the Cybercrime Office of the Florida Department of Law Enforcement of a reported incident;
- Requires CSOC to immediately notify the state CIO and the state cyber security information officer of a reported incident;
- Classifies certain IT security personnel as select exempt;
- Authorizes DMS to brief legislative committees on cybersecurity matters in a closed setting; and
- Requires that one of the three representatives on the Cybersecurity Advisory Council (CAC) from the critical infrastructure sectors must be from a utility provider and requires that one of the members of the CAC is a representative from a local government.

The bill does not have a fiscal impact on state or local government revenues or local government expenditures. The bill may increase state expenditures. *See* Fiscal Analysis & Economic Impact Statement.

The bill provides an effective date of July 1, 2024.

FULL ANALYSIS

I. SUBSTANTIVE ANALYSIS

A. EFFECT OF PROPOSED CHANGES:

Current Situation

Over the last decade, cybersecurity has rapidly become a growing concern. Cyberattacks are growing in frequency and severity. Cybercrime was expected to inflict $8 trillion worth of damage globally in 2023.[1] The United States is often a target of cyberattacks, including attacks on critical infrastructure, and has been a target of more significant cyberattacks[2] over the last 14 years than any other country.[3] The Colonial Pipeline is an example of critical infrastructure that was attacked, disrupting what is arguably the nation's most important fuel conduit.[4]

Ransomware is a type of cybersecurity incident where malware[5] that is designed to encrypt files on a device renders the files and the systems that rely on them unusable. In other words, critical information is no longer accessible. During a ransomware attack, malicious actors demand a ransom in exchange for regained access through decryption. If the ransom is not paid, the ransomware actors will often threaten to sell or leak the data or authentication information. Even if the ransom is paid, there is no guarantee that the bad actor will follow through with decryption.

In recent years, ransomware incidents have become increasingly prevalent among the nation's state, local, tribal, and territorial government entities and critical infrastructure organizations.[6] For example, Tallahassee Memorial Hospital was hit by a ransomware attack early in 2023, and the hospital's systems were forced to shut down, impacting many local residents in need of medical care.[7] Likewise, Tampa General Hospital detected a data breach in May of 2023, which may have compromised the data of up to 1.2 million patients.[8]

IT and Cybersecurity Management

The Department of Management Services (DMS) oversees information technology (IT)[9] governance and security for the executive branch in Florida.[10] The Florida Digital Service (FLDS) is housed within

---

[1] Cybercrime Magazine, *Cybercrime to Cost the World $8 Trillion Annually in 2023*, https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/ (last visited Jan. 23, 2024).
[2] "Significant cyber-attacks" are defined as cyber-attacks on a country's government agencies, defense, and high-tech companies, or economic crimes with losses equating to more than a million dollars. FRA Conferences, *Study: U.S. Largest Target for Significant Cyber-Attacks*, https://www.fraconferences.com/insights-articles/compliance/study-us-largest-target-for-significant-cyber-attacks/#:~:text=The%20United%20States%20has%20been%20on%20the%20receiving,article%20is%20from%20FRA%27s%20sister%20company%2C%20Compliance%20Week (last visited Jan. 23, 2024).
[3] *Id*.
[4] S&P Global, *Pipeline operators must start reporting cyberattacks to government: TSA orders*, https://www.spglobal.com/commodityinsights/en/market-insights/latest-news/electric-power/052721-pipeline-operators-must-start-reporting-cyberattacks-to-government-tsa-orders?utm_campaign=corporatepro&utm_medium=contentdigest&utm_source=esgmay2021 (last visited Jan. 23, 2024).
[5] "Malware" means hardware, firmware, or software that is intentionally included or inserted in a system for a harmful purpose. https://csrc.nist.gov/glossary/term/malware (last visited Jan. 23, 2024).
[6] Cybersecurity and Infrastructure Agency, *Ransomware 101,* https://www.cisa.gov/stopransomware/ransomware-101 (last visited Jan. 23, 2024).
[7] Tallahassee Democrat, *TMH says it has taken 'major step' toward restoration after cybersecurity incident* (Feb. 15, 2023) https://www.tallahassee.com/story/news/local/2023/02/14/tmh-update-hospital-has-taken-major-step-toward-restoration/69904510007/ (last visited Jan. 23, 2023).
[8] Alessandro Mascellino, Infosecurity Magazine, *Tampa General Hospital Data Breach Impacts 1.2 Million Patients* (Jul. 24, 2023), https://www.infosecurity-magazine.com/news/tampa-hospital-data-breach/ (last visited Jan. 24, 2023).
[9] The term "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. S. 282.0041(19), F.S.
[10] *See* s. 20.22, F.S.

DMS and was established in 2020 to replace the Division of State Technology.[11] FLDS works under DMS to implement policies for IT and cybersecurity for state agencies.[12]
The head of FLDS is appointed by the Secretary of Management Services[13] and serves as the state chief information officer (CIO).[14] The CIO must have at least five years of experience in the development of IT system strategic planning and IT policy and, preferably, have leadership-level experience in the design, development, and deployment of interoperable software and data solutions.[15] FLDS must propose innovative solutions that securely modernize state government, including technology and information services, to achieve value through digital transformation and interoperability, and to fully support Florida's cloud first policy.[16]

DMS, through FLDS, has the following powers, duties, and functions:

- Develop IT policy for the management of the state's IT resources;
- Develop an enterprise architecture;
- Establish project management and oversight standards with which state agencies must comply when implementing IT projects;
- Perform project oversight on all state agency IT projects that have a total cost of $10 million or more and that are funded in the General Appropriations Act or any other law; and
- Identify opportunities for standardization and consolidation of IT services that support interoperability, Florida's cloud first policy, and business functions and operations that are common across state agencies.[17]

State Cybersecurity Act

In 2021, the Legislature passed the State Cybersecurity Act,[18] which requires DMS and the heads of the state agencies[19] to meet certain requirements to enhance the cybersecurity[20] of the state agencies. DMS is tasked with completing the following, through FLDS:

- Establishing standards for assessing agency cybersecurity risks;
- Adopting rules to mitigate risk, support a security governance framework, and safeguard agency digital assets, data,[21] information, and IT resources;[22]
- Designating a chief information security officer (CISO);
- Developing and annually updating a statewide cybersecurity strategic plan to address matters such as identification and mitigation of risk, protections against threats, and tactical risk detection for cyber incidents;[23]
- Developing and publishing for use by state agencies a cybersecurity governance framework;
- Assisting the state agencies in complying with the State Cybersecurity Act;
- Annually providing training on cybersecurity for managers and team members;
- Annually reviewing the strategic and operational cybersecurity plans of state agencies;
- Tracking the state agencies' implementation of remediation plans;

---

[11] Ch. 2020-161, L.O.F.
[12] *See* s. 20.22(2)(b), F.S.
[13] The Secretary of Management Services serves as the head of DMS and is appointed by the Governor, subject to confirmation by the Senate. S. 20.22(1), F.S.
[14] S. 282.0051(2)(a), F.S.
[15] *Id.*
[16] S. 282.0051(1), F.S.
[17] *Id*.
[18] Ch. 2012-234, L.O.F.
[19] For purposes of the State Cybersecurity Act, the term "state agency" includes the Department of Legal Affairs, the Department of Agriculture and Consumer Services, and the Department of Financial Services. S. 282.318(2), F.S.
[20] "Cybersecurity" means 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 IT resources. S. 282.0041(8), F.S.
[21] "Data" means a subset of structured information in a format that allows such information to be electronically retrieved and transmitted. S. 282.0041(9), F.S.
[22] "Information technology resources" means data processing hardware and software and services, communications, supplies, personnel, facility resources, maintenance, and training. S. 282.0041(22), F.S.
[23] "Incident" means a violation or imminent threat of violation, whether such violation is accidental or deliberate, of IT resources, security, policies, or practices. An imminent threat of violation refers to a situation in which the state agency has a factual basis for believing that a specific incident is about to occur. S. 282.0041(19), F.S.

- Providing cybersecurity training to all state agency technology professionals that develops, assesses, and documents competencies by role and skill level;
- Maintaining a Cybersecurity Operations Center (CSOC) led by the CISO to serve as a clearinghouse for threat information and coordinate with FDLE to support responses to incidents; and
- Leading an Emergency Support Function under the state emergency management plan.[24]

The State Cybersecurity Act requires the head of each state agency to designate an information security manager to administer the state agency's cybersecurity program.[25] The head of the agency has additional tasks in protecting against cybersecurity threats as follows:

- Establish a cybersecurity incident response team with FLDS and the Cybercrime Office in FDLE, which must immediately report all confirmed or suspected incidents to the CISO;
- Annually submit to DMS the state agency's strategic and operational cybersecurity plans;
- Conduct and update a comprehensive risk assessment to determine the security threats;
- Develop and update written internal policies and procedures for reporting cyber incidents;
- Implement safeguards and risk assessment remediation plans to address identified risks;
- Ensure internal audits and evaluations of the agency's cybersecurity program are conducted;
- Ensure that the cybersecurity requirements for the solicitation, contracts, and service-level agreement of IT and IT resources meet or exceed applicable state and federal laws, regulations, and standards for cybersecurity, including the National Institute of Standards and Technology (NIST)[26] cybersecurity framework;
- Provide cybersecurity training to all agency employees within 30 days of employment; and
- Develop a process that is consistent with the rules and guidelines established by FLDS for detecting, reporting, and responding to threats, breaches, or cybersecurity incidents.[27]

Florida Cybersecurity Advisory Council

The Florida Cybersecurity Advisory Council[28] (CAC) within DMS[29] assists state agencies in protecting IT resources from cyber threats and incidents.[30] The CAC must assist FLDS in implementing best cybersecurity practices, taking into consideration the final recommendations of the Florida Cybersecurity Task Force – a task force created to review and assess the state's cybersecurity infrastructure, governance, and operations.[31] The CAC meets at least quarterly to:

- Review existing state agency cybersecurity policies;
- Assess ongoing risks to state agency IT;
- Recommend a reporting and information sharing system to notify state agencies of new risks;
- Recommend data breach simulation exercises;
- Assist FLDS in developing cybersecurity best practice recommendations; and
- Examine inconsistencies between state and federal law regarding cybersecurity.[32]

---

[24] Ch. 2021-234, L.O.F.
[25] S. 282.318(4)(a), F.S.
[26] NIST, otherwise known as the National Institute of Standards and Technology, "is a non-regulatory government agency that develops technology, metrics, and standards to drive innovation and economic competitiveness at U.S.-based organizations in the science and technology industry." Nate Lord, *What is NIST Compliance*, DataInsider (Dec. 1, 2020), https://www.digitalguardian.com/blog/what-nist-compliance (last visited Jan. 23, 2024).
[27] S. 282.318(4), F.S.
[28] The CAC is comprised of: the Lieutenant Governor or his or her designee; the state CIO; the state chief information security officer; the director of the Division of Emergency Management or his or her designee; a representative of the computer crime center of the Department of Law Enforcement, appointed by the executive director of the Department of Law Enforcement; a representative of the Florida Fusion Center of the Department of Law Enforcement, appointed by the executive director of the Department of Law Enforcement; the Chief Inspector General; up to two representatives from institutions of higher education located in this state, appointed by the Governor; three representatives from critical infrastructure sectors, one of whom must be from a water treatment facility, appointed by the Governor; four representatives of the private sector with senior level experience in cybersecurity or software engineering from within the finance, energy, health care, and transportation sectors, appointed by the Governor; and two representatives with expertise on emerging technology, with one appointed by the President of the Senate and one appointed by the Speaker of the House of Representatives. S, 282.319(3), F.S.
[29] S. 282.319(1), F.S.
[30] S. 282.319(2), F.S.
[31] S. 282.319(3), F.S.
[32] S. 282.319(9), F.S.

The CAC must work with NIST and other federal agencies, private sector businesses, and private security experts to identify which local infrastructure sectors, not covered by federal law, are at the greatest risk of cyber-attacks and to identify categories of critical infrastructure as critical cyber infrastructure if cyber damage to the infrastructure could result in catastrophic consequences.[33]

The CAC must also prepare and submit a comprehensive report to the Governor, the President of the Senate, and the Speaker of the House of Representatives that includes data, trends, analysis, findings, and recommendations for state and local action regarding ransomware incidents that includes:

- Descriptive statistics, including the amount of ransom requested, duration of the incident, and overall monetary cost to taxpayers of the incident;
- A detailed statistical analysis of the circumstances that led to the ransomware incident which does not include the name of the state agency or local government, network information, or system identifying information;
- Statistical analysis of the level of cybersecurity employee training and frequency of data backup for the state agencies or local governments that reported incidents;
- Specific issues identified with current policy, procedure, rule, or statute and recommendations to address those issues; and
- Other recommendations to prevent ransomware incidents.

Cyber Incident Response

The National Cyber Incident Response Plan (NCIRP) was developed according to the direction of Presidential Policy Directive-41,[34] by the U.S. Department of Homeland Security. The NCIRP is part of the broader National Preparedness System and establishes the strategic framework for a whole-of-Nation approach to mitigating, responding to, and recovering from cybersecurity incidents posing risk to critical infrastructure.[35] The NCIRP was developed in coordination with federal, state, local, and private sector entities and is designed to interface with industry best practice standards for cybersecurity, including the NIST Cybersecurity Framework.

The NCIRP adopted a schema for describing the severity of cybersecurity incidents affecting the U.S. The schema establishes a common framework to evaluate and assess cybersecurity incidents to ensure that all departments and agencies have a common view of the severity of a given incident; urgency required for responding to a given incident; seniority level necessary for coordinating response efforts; and level of investment required for response efforts.[36]

The severity level of a cybersecurity incident in accordance with the NCIRP is determined as follows:

- Level 5: An emergency-level incident within the specified jurisdiction if the incident poses an imminent threat to the provision of wide-scale critical infrastructure services; national, state, or local security; or the lives of the country's, state's, or local government's citizens.
- Level 4: A severe-level incident if the incident is likely to result in a significant impact within the affected jurisdiction which affects the public health or safety; national, state, or local security; economic security; or individual civil liberties.
- Level 3: A high-level incident if the incident is likely to result in a demonstrable impact in the affected jurisdiction to public health or safety; national, state, or local security; economic security; civil liberties; or public confidence.
- Level 2: A medium-level incident if the incident may impact public health or safety; national, state, or local security; economic security; civil liberties; or public confidence.

[33] S. 282.319(10), F.S.
[34] Annex for PPD-41: *U.S. Cyber Incident Coordination*, available at: https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/annex-presidential-policy-directive-united-states-cyber-incident (last visited Jan. 23, 2024).
[35] Cybersecurity & Infrastructure Security Agency, *Cybersecurity Incident Response*, available at https://www.cisa.gov/topics/cybersecurity-best-practices/organizations-and-cyber-safety/cybersecurity-incident-response#:~:text=%20National%20Cyber%20Incident%20Response%20Plan%20%28NCIRP%29%20The,incidents%20and%20how%20those%20activities%20all%20fit%20together (last visited Jan. 23, 2024).
[36] *Id.*

- Level 1: A low-level incident if the incident is unlikely to impact public health or safety; national, state, or local security; economic security; or public confidence.[37]

State agencies and local governments in Florida, must report all ransomware incidents and any cybersecurity incidents at severity levels 3, 4, and 5 as soon as possible to the CSOC, but no later than 48 hours after discovery of a cybersecurity incident and no later than 12 hours after discovery of a ransomware incident.[38] CSOC must notify the President of the Senate and the Speaker of the House of Representatives of any severity level 3, 4, or 5 incident as soon as possible, but no later than 12 hours after receiving the incident report from the state agency or local government.[39] For state agency incidents at severity levels 1 and 2, the agency or local government must report these incidents to CSOC and the Cybercrime Office at FDLE as soon as possible.[40]

The notification must include a high-level description of the incident and the likely effects. An incident report for a cybersecurity or ransomware incident by a state agency or local government must include, at a minimum:

- A summary of the facts surrounding the cybersecurity or ransomware incident;
- The date on which the state agency or local government most recently backed up its data, the physical location of the backup, if the backup was affected, and if the backup was created using cloud computing;
- The types of data compromised by the cybersecurity or ransomware incident;
- The estimated fiscal impact of the cybersecurity or ransomware incident;
- In the case of a ransomware incident, the details of the ransom demanded; and
- If the reporting entity is a local government, a statement requesting or declining assistance from CSOC, FDLE Cybercrime Office, or sheriff.[41]

In addition, CSOC must provide consolidated incident reports to the President of the Senate, Speaker of the House of Representatives, and the CAC on a quarterly basis.[42] The consolidated incident reports to the CAC may not contain any state agency or local government name, network information, or system identifying information, but must contain sufficient relevant information to allow the CAC to fulfill its responsibilities.[43]

State agencies and local governments must submit an after-action report to FLDS within one week of the remediation of a cybersecurity or ransomware incident.[44] The report must summarize the incident, state the resolution, and any insights from the incident.

Effect of the Bill

Definitions

The bill provides the following definitions:

- "As a service" means the contracting with or outsourcing to a third party of a defined role or function as a means of delivery.
- "Cloud provider" means an entity that provides cloud-computing services.

The bill also defines “enterprise digital data” as information held by a state agency in electronic form that is deemed to be data owned by the state and held for state purposes by the state agency. The bill provides that enterprise digital data that is subject to statutory requirements for particular types of sensitive data or to contractual limitations for data marked as trade secrets or sensitive corporate data held by state agencies shall be treated in accordance with such requirements or limitations. Under the

[37] S. 282.318(3)(c)9.a, F.S.
[38] S. 282.318(3)(c)9.c, F.S.
[39] S. 282.318(3)(c)9.c.(II), F.S.
[40] S. 282.318(3)(c)(9)(d), F.S.
[41] S. 282.318(3)(c)9.b, F.S.
[42] S. 282.318(3)(c)9.e, F.S.
[43] *Id*.
[44] S. 282.318(4)(k), F.S.

bill, DMS must maintain personnel with appropriate licenses, certifications, or classifications to steward such enterprise digital data, as necessary.

DMS and FLDS Duties

The bill revises the duties of FLDS to include:

- Leading enterprise IT and cybersecurity efforts.
- Safeguarding enterprise digital data.
- Testing, developing, and deploying innovative solutions that securely modernize state government.

The bill provides that the state CIO, in consultation with the Secretary of DMS, must designate a state chief technology officer who is responsible for the following:

- Establishing and maintaining an enterprise architecture framework that ensures IT investments align with the state's strategic objectives and initiatives.
- Conducting comprehensive evaluations of potential technological solutions and cultivating strategic partnerships, internally with state enterprise agencies and externally with the private sector, to leverage collective expertise, foster collaboration, and advance the state's technological capabilities.
- Supervising program management of certain enterprise IT initiatives; providing advisory support and oversight for technology-related projects; and continuously identifying and recommending best practices to optimize outcomes of technology projects and enhance the enterprise's technological efficiency and effectiveness.

Under the bill, all confirmed or suspected incidents or threats to state IT resources must be reported by the state CIO, in consultation with the state CISO, to the Governor.

The bill provides that chief information security officers, information security managers, and personnel employed by or reporting to the state CIO, the state chief data officer, or an agency information security manager are designated as Selected Exempt Service and that the salary and benefits for these positions will be set accordingly.[45] The bill provides that DMS shall set the salary and benefits of the state chief technology officer in accordance with the rules of the Senior Management Service.[46]

The bill requires FLDS to ensure project oversight independent of the state agency on all state agency IT projects that have a total project cost of $25 million or more (up from $10 million per current law), and that the projects are performed in compliance with applicable state and federal law. The bill provides that when FLDS ensures performance of its project oversight function for the Department of Financial Services, the Department of Legal Affairs, or the Department of Agriculture and Consumer Services, FLDS must report within 30 days after the end of each quarter on any IT projects that FLDS identifies as high-risk.

Under the bill, FLDS no longer must conduct annual assessments of state agencies to determine compliance with all IT standards and guidelines developed and published by DMS. The bill removes a prohibition on FLDS retrieving or disclosing any data without a shared data agreement in place between DMS and the enterprise entity that has primary custodial responsibility of, or data sharing responsibility for, that data. The bill gives FLDS the authority to obtain immediate access to public or private infrastructure hosting enterprise digital data and to direct, in consultation with the state agency that holds the particular data, measures to assess, monitor, and safeguard such data.

The bill provides that DMS may brief any legislative committee or subcommittee responsible for cybersecurity policy in a meeting or other setting closed by the respective body. Such legislative committee or subcommittee must maintain the confidential and exempt status of records made

[45] The Selected Exempt Service is a separate system of personnel administration for specified positions in state government. S. 110.602, F.S.

[46] The Senior Management Service is created as a separate system of personnel administration for positions in the executive branch the duties and responsibilities of which are primarily and essentially policymaking or managerial in nature. S. 110.402(1), F.S.

confidential and exempt under current law. The bill states that a legislator serving on such legislative committee or subcommittee may also attend meetings of the Florida Cybersecurity Advisory Council.

Cybersecurity Operations Center Duties (CSOC)

The bill creates a new reporting requirement for CSOC. Under the bill, CSOC must immediately notify the Cybercrime Office of FDLE of a reported incident and provide regular reports on the status of the incident, preserve forensic data to support the subsequent investigation, and provide aid to the investigative efforts of the Cybercrime Office, upon request, if the state CISO finds that the investigation does not impede remediation of the incident and that there is no risk to the public and no risk to critical state functions.

Under the bill, the CSOC must also immediately notify the state CIO and the state CISO of a reported incident. The bill requires that the state CISO notify the President of the Senate and the Speaker of the House of Representatives within 24 hours after receiving report of the incident and the notification must be provided in a secure environment. The bill requires that within 30 days after the end of each quarter, CSOC must provide a consolidated incident report to the Governor, Attorney General, the executive director of the Department of Law Enforcement, President of the Senate, Speaker of the House of Representatives, and the CAC.

State Agency Duties

The bill requires state agencies to report all ransomware incidents, regardless of severity level, to CSOC as soon as possible, but no later than 12 hours after a cybersecurity incident and no later than 6 hours after the discovery of a ransomware incident.

The bill requires each state agency to designate a chief information security officer to integrate the agency's technical and operational cybersecurity efforts with CSOC. The bill requires that each agency shall provide this designation to the FLDS annually in writing. Each agency's designated chief information security officer is under the supervision of the given agency's department head for administrative purposes but must report to the state CISO. An agency may request that DMS procure a chief information security officer as a service to fulfill the agency's duty to designate one. Under the bill, each agency's information security manager must coordinate with the agency's chief information security officer and CSOC and ensure compliance with cybersecurity governance and with the state's enterprise security program and incident response plan.

Florida Cybersecurity Advisory Council (CAC)

The bill requires that one of the three representatives on the CAC from the critical infrastructure sectors must be from a utility provider. The bill removes the requirement that one CAC member must be from a water treatment facility. The bill also adds a requirement that one of the members of the CAC is a representative from a local government.

Local Government Duties

The bill removes the requirement that a local government must report any cybersecurity incident determined to be level 3, 4, or 5 to the Cybercrime Office of FDLE and the sheriff who has jurisdiction over the local government. The bill requires a local government to report a cybersecurity incident to CSOC within 12 hours of discovery and to report a ransomware incident within 6 hours after discovery.

Under the bill, after CSOC receives a report of a cybersecurity or ransomware incident, CSOC must immediately notify the Cybercrime Office of FDLE and the sheriff who has jurisdiction over the local government. CSOC must provide these entities with regular reports on the status of the incident, preserve forensic data to support a subsequent investigation, and provide aid to the investigative efforts of the Cybercrime Office upon the office's request if the state CISO finds that the investigation does not impede remediation of the incident and that there is no risk to the public and no risk to critical state functions. The bill also requires that CSOC immediately notify the state CISO of the reported incident.

The state CISO shall notify the President of the Senate and the Speaker of the House of Representatives no later than 24 hours after receiving report of the incident and must do so in a secure environment.

Under the bill, if CSOC receives a report from a local government of a level 1 or 2 cybersecurity incident, CSOC must immediately notify the Cybercrime Office and the sheriff who has jurisdiction over the local government, and CSOC shall provide regular reports on the status of the incident, preserve forensic data to support a subsequent investigation, and provide aid to the investigative efforts of the Cybercrime Office upon the office's request if the state CISO finds that the investigation does not impede remediation of the incident and that there is no risk to the public and no risk to critical state functions.

The bill provides an effective date of July 1, 2024.

B. SECTION DIRECTORY:

Section 1: Amends s. 110.205, F.S., relating to career service; exemptions.

Section 2: Amends s. 282.0041, F.S., relating to definitions.

Section 3: Amends s. 282.0051, F.S., relating to Department of Management Services; Florida Digital Service; power, duties, and functions.

Section 4: Amends s. 282.00515, F.S., relating to duties of cabinet agencies.

Section 5: Amends s. 282.318, F.S., relating to cybersecurity.

Section 6: Amends s. 282.3185, F.S., relating to local government cybersecurity.

Section 7: Amends s. 282.319, F.S., relating to Florida Cybersecurity Advisory Council.

Section 8: Provides an effective date.

II. FISCAL ANALYSIS & ECONOMIC IMPACT STATEMENT

A. FISCAL IMPACT ON STATE GOVERNMENT:

1. Revenues:

   None.

2. Expenditures:

   Indeterminate. The bill may increase state expenditures because it elevates state agency CISO's, information security managers and other related personnel to Selected Exempt Service status and requires each state agency to designate a chief information security officer.

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 require counties or municipalities to spend funds or take action requiring the expenditures 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:

None.

B. RULE-MAKING AUTHORITY:

The bill does not require or authorize rulemaking.

C. DRAFTING ISSUES OR OTHER COMMENTS:

None.

IV. AMENDMENTS/COMMITTEE SUBSTITUTE CHANGES

Not applicable.

A bill to be entitled

An act relating to cybersecurity; amending s. 110.205, F.S.; exempting certain personnel from the career service; providing for the establishment of salary and benefits for certain positions; amending s. 282.0041, F.S.; providing definitions; amending s. 282.0051, F.S.; revising the purposes for which the Florida Digital Service is established; requiring the Florida Digital Service to ensure that independent project oversight on certain state agency information technology projects is performed in a certain manner; revising the date by which the Department of Management Services, acting through the Florida Digital Service, must provide certain recommendations to the Executive Office of the Governor and the Legislature; removing certain duties of the Florida Digital Service; revising the total project cost of certain projects for which the Florida Digital Service must provide project oversight; specifying the date by which the Florida Digital Service must provide certain reports; requiring the state chief information officer, in consultation with the Secretary of Management Services, to designate a state chief technology officer; providing duties of the state chief technology officer; revising the total project

cost of certain projects for which certain procurement actions must be taken; removing provisions prohibiting the department, acting through the Florida Digital Service, from retrieving or disclosing certain data in certain circumstances; amending s. 282.00515, F.S.; conforming a cross-reference; amending s. 282.318, F.S.; providing that the Florida Digital Service is the lead entity for a certain purpose; requiring the Cybersecurity Operations Center to provide certain notifications; requiring the state chief information officer to make certain reports in consultation with the state chief information security officer; requiring a state agency to report ransomware and cybersecurity incidents within certain time periods; requiring the Cybersecurity Operations Center to immediately notify certain entities of reported incidents and take certain actions; requiring the state chief information security officer to notify the Legislature of certain incidents within a certain period; requiring certain notification to be provided in a secure environment; requiring the Cybersecurity Operations Center to provide a certain report to certain entities by a specified date; requiring the Florida Digital Service to provide cybersecurity briefings to certain legislative committees;

authorizing the Florida Digital Service to obtain certain access to certain infrastructure and direct certain measures; requiring a state agency head to annually designate a chief information security officer by a specified date; revising the purpose of an agency's information security manager and the date by which he or she must be designated; authorizing the department to brief certain legislative committees in a closed setting on certain records that are confidential and exempt from public records requirements; requiring such legislative committees to maintain the confidential and exempt status of certain records; authorizing certain legislators to attend meetings of the Florida Cybersecurity Advisory Council; amending s. 282.3185, F.S.; requiring a local government to report ransomware and certain cybersecurity incidents to the Cybersecurity Operations Center within certain time periods; requiring the Cybersecurity Operations Center to immediately notify certain entities of certain incidents and take certain actions; requiring certain notification to be provided in a secure environment; amending s. 282.319, F.S.; revising the membership of the Florida Cybersecurity Advisory Council; providing an effective date.

Be It Enacted by the Legislature of the State of Florida:

Section 1. Paragraph (e) of subsection (2) of section 110.205, Florida Statutes, is amended, and paragraph (y) is added to subsection (2) of that section, to read:

110.205 Career service; exemptions.—

(2) EXEMPT POSITIONS.—The exempt positions that are not covered by this part include the following:

(e) The state chief information officer, the state chief data officer, the state chief technology officer, and the state chief information security officer. The Department of Management Services shall set the salary and benefits of these positions in accordance with the rules of the Senior Management Service.

(y) Chief information security officers, information security managers designated pursuant to s. 282.318(4), and personnel employed by or reporting to the state chief information security officer, the state chief data officer, or an agency information security manager. Unless otherwise fixed by law, the department shall establish the salary and benefits for these positions in accordance with the rules of the Selected Exempt Service, except that the salary and benefits for the agency information security manager shall be established by the department in accordance with the rules of the Senior Management Service.

Section 2. Subsections (3) through (5), (6) through (16), and (17) through (38) of section 282.0041, Florida Statutes, are renumbered as subsections (4) through (6), (8) through (18), and (20) through (41), respectively, and new subsections (3), (7), and (19) are added to that section to read:

282.0041 Definitions.—As used in this chapter, the term:

(3) "As a service" means the contracting with or outsourcing to a third party of a defined role or function as a means of delivery.

(7) "Cloud provider" means an entity that provides cloud-computing services.

(19) "Enterprise digital data" means information held by a state agency in electronic form that is deemed to be data owned by the state and held for state purposes by the state agency. Enterprise digital data that is subject to statutory requirements for particular types of sensitive data or to contractual limitations for data marked as trade secrets or sensitive corporate data held by state agencies shall be treated in accordance with such requirements or limitations. The department must maintain personnel with appropriate licenses, certifications, or classifications to steward such enterprise digital data, as necessary. Enterprise digital data must be maintained in accordance with chapter 119. This subsection may not be construed to create or expand an exemption from public records requirements under s. 119.07(1) or s. 24(a), Art. I of

the State Constitution.

Section 3. Subsection (6) of section 282.0051, Florida Statutes, is renumbered as subsection (5), subsections (1) and (4) and present subsection (5) are amended, and paragraph (c) is added to subsection (2) of that section, to read:

282.0051 Department of Management Services; Florida Digital Service; powers, duties, and functions.—

(1) The Florida Digital Service is established ~~has been created~~ within the department to lead enterprise information technology and cybersecurity efforts, to safeguard enterprise digital data, to propose, test, develop, and deploy innovative solutions that securely modernize state government, including technology and information services, to achieve value through digital transformation and interoperability, and to fully support the cloud-first policy as specified in s. 282.206. The department, through the Florida Digital Service, shall have the following powers, duties, and functions:

(a) Develop and publish information technology policy for the management of the state's information technology resources.

(b) Develop an enterprise architecture that:

1. Acknowledges the unique needs of the entities within the enterprise in the development and publication of standards and terminologies to facilitate digital interoperability;

2. Supports the cloud-first policy as specified in s. 282.206; and

3. Addresses how information technology infrastructure may be modernized to achieve cloud-first objectives.

(c) Establish project management and oversight standards with which state agencies must comply when implementing information technology projects. The department, acting through the Florida Digital Service, shall provide training opportunities to state agencies to assist in the adoption of the project management and oversight standards. To support data-driven decisionmaking, the standards must include, but are not limited to:

1. Performance measurements and metrics that objectively reflect the status of an information technology project based on a defined and documented project scope, cost, and schedule.

2. Methodologies for calculating acceptable variances in the projected versus actual scope, schedule, or cost of an information technology project.

3. Reporting requirements, including requirements designed to alert all defined stakeholders that an information technology project has exceeded acceptable variances defined and documented in a project plan.

4. Content, format, and frequency of project updates.

5. Technical standards to ensure an information technology project complies with the enterprise architecture.

(d) Ensure that independent ~~Perform~~ project oversight on all state agency information technology projects that have total

project costs of $25 ~~$10~~ million or more and that are funded in the General Appropriations Act or any other law is performed in compliance with applicable state and federal law. The department, acting through the Florida Digital Service, shall report at least quarterly to the Executive Office of the Governor, the President of the Senate, and the Speaker of the House of Representatives on any information technology project that the department identifies as high-risk due to the project exceeding acceptable variance ranges defined and documented in a project plan. The report must include a risk assessment, including fiscal risks, associated with proceeding to the next stage of the project, and a recommendation for corrective actions required, including suspension or termination of the project.

(e) Identify opportunities for standardization and consolidation of information technology services that support interoperability and the cloud-first policy, as specified in s. 282.206, and business functions and operations, including administrative functions such as purchasing, accounting and reporting, cash management, and personnel, and that are common across state agencies. The department, acting through the Florida Digital Service, shall biennially on January 15 ~~1~~ of each even-numbered year provide recommendations for standardization and consolidation to the Executive Office of the Governor, the President of the Senate, and the Speaker of the

House of Representatives.

(f) Establish best practices for the procurement of information technology products and cloud-computing services in order to reduce costs, increase the quality of data center services, or improve government services.

(g) Develop standards for information technology reports and updates, including, but not limited to, operational work plans, project spend plans, and project status reports, for use by state agencies.

(h) Upon request, assist state agencies in the development of information technology-related legislative budget requests.

~~(i) Conduct annual assessments of state agencies to determine compliance with all information technology standards and guidelines developed and published by the department and provide results of the assessments to the Executive Office of the Governor, the President of the Senate, and the Speaker of the House of Representatives.~~

(i)~~(j)~~ Conduct a market analysis not less frequently than every 3 years beginning in 2021 to determine whether the information technology resources within the enterprise are utilized in the most cost-effective and cost-efficient manner, while recognizing that the replacement of certain legacy information technology systems within the enterprise may be cost prohibitive or cost inefficient due to the remaining useful life of those resources; whether the enterprise is complying with the

cloud-first policy specified in s. 282.206; and whether the enterprise is utilizing best practices with respect to information technology, information services, and the acquisition of emerging technologies and information services. Each market analysis shall be used to prepare a strategic plan for continued and future information technology and information services for the enterprise, including, but not limited to, proposed acquisition of new services or technologies and approaches to the implementation of any new services or technologies. Copies of each market analysis and accompanying strategic plan must be submitted to the Executive Office of the Governor, the President of the Senate, and the Speaker of the House of Representatives not later than December 31 of each year that a market analysis is conducted.

(j) ~~(k)~~ Recommend other information technology services that should be designed, delivered, and managed as enterprise information technology services. Recommendations must include the identification of existing information technology resources associated with the services, if existing services must be transferred as a result of being delivered and managed as enterprise information technology services.

(k) ~~(l)~~ In consultation with state agencies, propose a methodology and approach for identifying and collecting both current and planned information technology expenditure data at the state agency level.

(l) ~~(m)~~1. Notwithstanding any other law, provide project oversight on any information technology project of the Department of Financial Services, the Department of Legal Affairs, and the Department of Agriculture and Consumer Services which has a total project cost of $25 ~~$20~~ million or more. Such information technology projects must also comply with the applicable information technology architecture, project management and oversight, and reporting standards established by the department, acting through the Florida Digital Service.

2. When ensuring performance of ~~performing~~ the project oversight function specified in subparagraph 1., report by the 30th day after the end of each quarter ~~at least quarterly~~ to the Executive Office of the Governor, the President of the Senate, and the Speaker of the House of Representatives on any information technology project that the department, acting through the Florida Digital Service, identifies as high-risk due to the project exceeding acceptable variance ranges defined and documented in the project plan. The report shall include a risk assessment, including fiscal risks, associated with proceeding to the next stage of the project and a recommendation for corrective actions required, including suspension or termination of the project.

(m) ~~(n)~~ If an information technology project implemented by a state agency must be connected to or otherwise accommodated by an information technology system administered by the Department

of Financial Services, the Department of Legal Affairs, or the Department of Agriculture and Consumer Services, consult with these departments regarding the risks and other effects of such projects on their information technology systems and work cooperatively with these departments regarding the connections, interfaces, timing, or accommodations required to implement such projects.

(n) ~~(o)~~ If adherence to standards or policies adopted by or established pursuant to this section causes conflict with federal regulations or requirements imposed on an entity within the enterprise and results in adverse action against an entity or federal funding, work with the entity to provide alternative standards, policies, or requirements that do not conflict with the federal regulation or requirement. The department, acting through the Florida Digital Service, shall annually by January 15 report such alternative standards to the Executive Office of the Governor, the President of the Senate, and the Speaker of the House of Representatives.

(o) ~~(p)~~1. Establish an information technology policy for all information technology-related state contracts, including state term contracts for information technology commodities, consultant services, and staff augmentation services. The information technology policy must include:

a. Identification of the information technology product and service categories to be included in state term contracts.

b. Requirements to be included in solicitations for state term contracts.

c. Evaluation criteria for the award of information technology-related state term contracts.

d. The term of each information technology-related state term contract.

e. The maximum number of vendors authorized on each state term contract.

f. At a minimum, a requirement that any contract for information technology commodities or services meet the National Institute of Standards and Technology Cybersecurity Framework.

g. For an information technology project wherein project oversight is required pursuant to paragraph (d) or paragraph (l) ~~(m)~~, a requirement that independent verification and validation be employed throughout the project life cycle with the primary objective of independent verification and validation being to provide an objective assessment of products and processes throughout the project life cycle. An entity providing independent verification and validation may not have technical, managerial, or financial interest in the project and may not have responsibility for, or participate in, any other aspect of the project.

2. Evaluate vendor responses for information technology-related state term contract solicitations and invitations to negotiate.

3. Answer vendor questions on information technology-related state term contract solicitations.

4. Ensure that the information technology policy established pursuant to subparagraph 1. is included in all solicitations and contracts that are administratively executed by the department.

(p) ~~(q)~~ Recommend potential methods for standardizing data across state agencies which will promote interoperability and reduce the collection of duplicative data.

(q) ~~(r)~~ Recommend open data technical standards and terminologies for use by the enterprise.

(r) ~~(s)~~ Ensure that enterprise information technology solutions are capable of utilizing an electronic credential and comply with the enterprise architecture standards.

(2)

(c) The state chief information officer, in consultation with the Secretary of Management Services, shall designate a state chief technology officer who shall be responsible for all of the following:

1. Establishing and maintaining an enterprise architecture framework that ensures information technology investments align with the state's strategic objectives and initiatives pursuant to paragraph (1)(b).

2. Conducting comprehensive evaluations of potential technological solutions and cultivating strategic partnerships,

internally with state enterprise agencies and externally with the private sector, to leverage collective expertise, foster collaboration, and advance the state's technological capabilities.

3. Supervising program management of enterprise information technology initiatives pursuant to paragraphs (1)(c), (d), and (l); providing advisory support and oversight for technology-related projects; and continuously identifying and recommending best practices to optimize outcomes of technology projects and enhance the enterprise's technological efficiency and effectiveness.

(4) For information technology projects that have a total project cost of $25 ~~$10~~ million or more:

(a) State agencies must provide the Florida Digital Service with written notice of any planned procurement of an information technology project.

(b) The Florida Digital Service must participate in the development of specifications and recommend modifications to any planned procurement of an information technology project by state agencies so that the procurement complies with the enterprise architecture.

(c) The Florida Digital Service must participate in post-award contract monitoring.

~~(5) The department, acting through the Florida Digital Service, may not retrieve or disclose any data without a shared-~~

~~data agreement in place between the department and the enterprise entity that has primary custodial responsibility of, or data-sharing responsibility for, that data.~~

Section 4. Subsection (1) of section 282.00515, Florida Statutes, is amended to read:

282.00515 Duties of Cabinet agencies.—

(1) The Department of Legal Affairs, the Department of Financial Services, and the Department of Agriculture and Consumer Services shall adopt the standards established in s. 282.0051(1)(b), (c), and (q) ~~(r)~~ and (3)(e) or adopt alternative standards based on best practices and industry standards that allow for open data interoperability.

Section 5. Paragraphs (a) through (k) of subsection (4) of section 282.318, Florida Statutes, are redesignated as paragraphs (b) through (l), respectively, subsection (10) is renumbered as subsection (11), subsection (3) and present paragraph (a) of subsection (4) are amended, a new paragraph (a) is added to subsection (4), and a new subsection (10) is added to that section, to read:

282.318 Cybersecurity.—

(3) The ~~department, acting through the~~ Florida Digital Service~~,~~ is the lead entity responsible for leading enterprise information technology and cybersecurity efforts, safeguarding enterprise digital data, establishing standards and processes for assessing state agency cybersecurity risks, and determining

appropriate security measures. Such standards and processes must be consistent with generally accepted technology best practices, including the National Institute for Standards and Technology Cybersecurity Framework, for cybersecurity. The department, acting through the Florida Digital Service, shall adopt rules that mitigate risks; safeguard state agency digital assets, data, information, and information technology resources to ensure availability, confidentiality, and integrity; and support a security governance framework. The department, acting through the Florida Digital Service, shall also:

(a) Designate an employee of the Florida Digital Service as the state chief information security officer. The state chief information security officer must have experience and expertise in security and risk management for communications and information technology resources. The state chief information security officer is responsible for the development, operation, and oversight of cybersecurity for state technology systems. The Cybersecurity Operations Center shall immediately notify the state chief information officer and the state chief information security officer ~~shall be notified~~ of all confirmed or suspected incidents or threats of state agency information technology resources. The state chief information officer, in consultation with the state chief information security officer, ~~and~~ must report such incidents or threats to ~~the state chief information officer and~~ the Governor.

(b) Develop, and annually update by February 1, a statewide cybersecurity strategic plan that includes security goals and objectives for cybersecurity, including the identification and mitigation of risk, proactive protections against threats, tactical risk detection, threat reporting, and response and recovery protocols for a cyber incident.

(c) Develop and publish for use by state agencies a cybersecurity governance framework that, at a minimum, includes guidelines and processes for:

1. Establishing asset management procedures to ensure that an agency's information technology resources are identified and managed consistent with their relative importance to the agency's business objectives.

2. Using a standard risk assessment methodology that includes the identification of an agency's priorities, constraints, risk tolerances, and assumptions necessary to support operational risk decisions.

3. Completing comprehensive risk assessments and cybersecurity audits, which may be completed by a private sector vendor, and submitting completed assessments and audits to the department.

4. Identifying protection procedures to manage the protection of an agency's information, data, and information technology resources.

5. Establishing procedures for accessing information and

data to ensure the confidentiality, integrity, and availability of such information and data.

6. Detecting threats through proactive monitoring of events, continuous security monitoring, and defined detection processes.

7. Establishing agency cybersecurity incident response teams and describing their responsibilities for responding to cybersecurity incidents, including breaches of personal information containing confidential or exempt data.

8. Recovering information and data in response to a cybersecurity incident. The recovery may include recommended improvements to the agency processes, policies, or guidelines.

9. Establishing a cybersecurity incident reporting process that includes procedures for notifying the department and the Department of Law Enforcement of cybersecurity incidents.

a. The level of severity of the cybersecurity incident is defined by the National Cyber Incident Response Plan of the United States Department of Homeland Security as follows:

(I) Level 5 is an emergency-level incident within the specified jurisdiction that poses an imminent threat to the provision of wide-scale critical infrastructure services; national, state, or local government security; or the lives of the country's, state's, or local government's residents.

(II) Level 4 is a severe-level incident that is likely to result in a significant impact in the affected jurisdiction to

public health or safety; national, state, or local security; economic security; or civil liberties.

(III) Level 3 is a high-level incident that is likely to result in a demonstrable impact in the affected jurisdiction to public health or safety; national, state, or local security; economic security; civil liberties; or public confidence.

(IV) Level 2 is a medium-level incident that may impact public health or safety; national, state, or local security; economic security; civil liberties; or public confidence.

(V) Level 1 is a low-level incident that is unlikely to impact public health or safety; national, state, or local security; economic security; civil liberties; or public confidence.

b. The cybersecurity incident reporting process must specify the information that must be reported by a state agency following a cybersecurity incident or ransomware incident, which, at a minimum, must include the following:

(I) A summary of the facts surrounding the cybersecurity incident or ransomware incident.

(II) The date on which the state agency most recently backed up its data; the physical location of the backup, if the backup was affected; and if the backup was created using cloud computing.

(III) The types of data compromised by the cybersecurity incident or ransomware incident.

(IV) The estimated fiscal impact of the cybersecurity incident or ransomware incident.

(V) In the case of a ransomware incident, the details of the ransom demanded.

c.(I) A state agency shall report all ransomware incidents and ~~any~~ cybersecurity incidents ~~incident determined by the state agency to be of severity level 3, 4, or 5~~ to the Cybersecurity Operations Center ~~and the Cybercrime Office of the Department of Law Enforcement~~ as soon as possible but no later than 12 ~~48~~ hours after discovery of the cybersecurity incident and no later than 6 ~~12~~ hours after discovery of the ransomware incident. The report must contain the information required in sub-subparagraph b.

(II) The Cybersecurity Operations Center shall:

(A) Immediately notify the Cybercrime Office of the Department of Law Enforcement of a reported incident and provide to the Cybercrime Office of the Department of Law Enforcement regular reports on the status of the incident, preserve forensic data to support a subsequent investigation, and provide aid to the investigative efforts of the Cybercrime Office of the Department of Law Enforcement upon the office's request if the state chief information security officer finds that the investigation does not impede remediation of the incident and that there is no risk to the public and no risk to critical state functions.

(B) Immediately notify the state chief information officer and the state chief information security officer of a reported incident. The state chief information security officer shall notify the President of the Senate and the Speaker of the House of Representatives of any severity level 3, 4, or 5 incident as soon as possible but no later than 24 ~~12~~ hours after receiving a state agency's incident report. The notification must include a high-level description of the incident and the likely effects and must be provided in a secure environment.

~~d. A state agency shall report a cybersecurity incident determined by the state agency to be of severity level 1 or 2 to the Cybersecurity Operations Center and the Cybercrime Office of the Department of Law Enforcement as soon as possible. The report must contain the information required in sub-subparagraph b.~~

d.~~e.~~ The Cybersecurity Operations Center shall provide a consolidated incident report by the 30th day after the end of each quarter ~~on a quarterly basis~~ to the Governor, the Attorney General, the executive director of the Department of Law Enforcement, the President of the Senate, the Speaker of the House of Representatives, and the Florida Cybersecurity Advisory Council. The report provided to the Florida Cybersecurity Advisory Council may not contain the name of any agency, network information, or system identifying information but must contain sufficient relevant information to allow the Florida

Cybersecurity Advisory Council to fulfill its responsibilities as required in s. 282.319(9).

10. Incorporating information obtained through detection and response activities into the agency's cybersecurity incident response plans.

11. Developing agency strategic and operational cybersecurity plans required pursuant to this section.

12. Establishing the managerial, operational, and technical safeguards for protecting state government data and information technology resources that align with the state agency risk management strategy and that protect the confidentiality, integrity, and availability of information and data.

13. Establishing procedures for procuring information technology commodities and services that require the commodity or service to meet the National Institute of Standards and Technology Cybersecurity Framework.

14. Submitting after-action reports following a cybersecurity incident or ransomware incident. Such guidelines and processes for submitting after-action reports must be developed and published by December 1, 2022.

(d) Assist state agencies in complying with this section.

(e) In collaboration with the Cybercrime Office of the Department of Law Enforcement, annually provide training for state agency information security managers and computer security

incident response team members that contains training on cybersecurity, including cybersecurity threats, trends, and best practices.

(f) Annually review the strategic and operational cybersecurity plans of state agencies.

(g) Annually provide cybersecurity training to all state agency technology professionals and employees with access to highly sensitive information which develops, assesses, and documents competencies by role and skill level. The cybersecurity training curriculum must include training on the identification of each cybersecurity incident severity level referenced in sub-subparagraph (c)9.a. The training may be provided in collaboration with the Cybercrime Office of the Department of Law Enforcement, a private sector entity, or an institution of the State University System.

(h) Operate and maintain a Cybersecurity Operations Center led by the state chief information security officer, which must be primarily virtual and staffed with tactical detection and incident response personnel. The Cybersecurity Operations Center shall serve as a clearinghouse for threat information and coordinate with the Department of Law Enforcement to support state agencies and their response to any confirmed or suspected cybersecurity incident.

(i) Lead an Emergency Support Function, ESF-20 ~~ESF CYBER~~, under the state comprehensive emergency management plan as

described in s. 252.35.

(j) Provide cybersecurity briefings to the members of any legislative committee or subcommittee responsible for policy matters relating to cybersecurity.

(k) Have the authority to obtain immediate access to public or private infrastructure hosting enterprise digital data and to direct, in consultation with the state agency that holds the particular enterprise digital data, measures to assess, monitor, and safeguard the enterprise digital data.

(4) Each state agency head shall, at a minimum:

(a) Designate a chief information security officer to integrate the agency's technical and operational cybersecurity efforts with the Cybersecurity Operations Center. This designation must be provided annually in writing to the Florida Digital Service by January 15. For a state agency under the jurisdiction of the Governor, the agency's chief information security officer shall be under the general supervision of the agency head or designee for administrative purposes but shall report to the state chief information officer. An agency may request that the department procure a chief information security officer as a service to fulfill the agency's duties under this paragraph.

(b) ~~(a)~~ Designate an information security manager to ensure compliance with cybersecurity governance and with the state's enterprise security program and incident response plan. The

information security manager must coordinate with the agency's chief information security officer and the Cybersecurity Operations Center to ensure that the unique needs of the agency are met ~~administer the cybersecurity program of the state agency~~. This designation must be provided annually in writing to the department by January 15 ~~1~~. A state agency's information security manager, for purposes of these information security duties, shall work in collaboration with the agency's chief information security officer and report directly to the agency head.

(10) The department may brief any legislative committee or subcommittee responsible for cybersecurity policy in a meeting or other setting closed by the respective body under the rules of such legislative body at which the legislative committee or subcommittee is briefed on records made confidential and exempt under subsections (5) and (6). The legislative committee or subcommittee must maintain the confidential and exempt status of such records. A legislator serving on a legislative committee or subcommittee responsible for cybersecurity policy may also attend meetings of the Florida Cybersecurity Advisory Council, including any portions of such meetings that are exempt from s. 286.011 and s. 24(b), Art. I of the State Constitution.

Section 6. Paragraph (d) of subsection (5) of section 282.3185, Florida Statutes, is redesignated as paragraph (c), and paragraph (b) and present paragraph (c) of that subsection

are amended to read:

282.3185 Local government cybersecurity.—

(5) INCIDENT NOTIFICATION.—

(b)1. A local government shall report all ransomware incidents and any cybersecurity incident determined by the local government to be of severity level 3, 4, or 5 as provided in s. 282.318(3)(c) to the Cybersecurity Operations Center~~, the Cybercrime Office of the Department of Law Enforcement, and the sheriff who has jurisdiction over the local government~~ as soon as possible but no later than 12 ~~48~~ hours after discovery of the cybersecurity incident and no later than 6 ~~12~~ hours after discovery of the ransomware incident. The report must contain the information required in paragraph (a).

2. The Cybersecurity Operations Center shall:

a. Immediately notify the Cybercrime Office of the Department of Law Enforcement and the sheriff who has jurisdiction over the local government of a reported incident and provide to the Cybercrime Office of the Department of Law Enforcement and the sheriff who has jurisdiction over the local government regular reports on the status of the incident, preserve forensic data to support a subsequent investigation, and provide aid to the investigative efforts of the Cybercrime Office of the Department of Law Enforcement upon the office's request if the state chief information security officer finds that the investigation does not impede remediation of the

incident and that there is no risk to the public and no risk to critical state functions.

b. Immediately notify the state chief information security officer of a reported incident. The state chief information security officer shall notify the President of the Senate and the Speaker of the House of Representatives of any severity level 3, 4, or 5 incident as soon as possible but no later than 24 ~~12~~ hours after receiving a local government's incident report. The notification must include a high-level description of the incident and the likely effects and must be provided in a secure environment.

(c) A local government may report a cybersecurity incident determined by the local government to be of severity level 1 or 2 as provided in s. 282.318(3)(c) to the Cybersecurity Operations Center, the Cybercrime Office of the Department of Law Enforcement, and the sheriff who has jurisdiction over the local government. The report shall contain the information required in paragraph (a). The Cybersecurity Operations Center shall immediately notify the Cybercrime Office of the Department of Law Enforcement and the sheriff who has jurisdiction over the local government of a reported incident and provide regular reports on the status of the cybersecurity incident, preserve forensic data to support a subsequent investigation, and provide aid to the investigative efforts of the Cybercrime Office of the Department of Law Enforcement upon request if the state chief

information security officer finds that the investigation does not impede remediation of the cybersecurity incident and that there is no risk to the public and no risk to critical state functions.

Section 7. Paragraph (j) of subsection (4) of section 282.319, Florida Statutes, is amended, and paragraph (m) is added to that subsection, to read:

282.319 Florida Cybersecurity Advisory Council.—

(4) The council shall be comprised of the following members:

(j) Three representatives from critical infrastructure sectors, one of whom must be from a utility provider ~~water treatment facility~~, appointed by the Governor.

(m) A representative of local government.

Section 8. This act shall take effect July 1, 2024.

Energy, Communications & Cybersecurity Subcommittee
HB 1555 by Rep. Giallombardo
Cybersecurity

AMENDMENT SUMMARY
January 25, 2024

Amendment 1 by Giallombardo (line 90):

- Removes provisions of the bill that designate certain information security personnel positions as select exempt positions.

Amendment 2 by Giallombardo (line 611):

- Removes provisions of the bill that require each state agency head to designate a chief information security officer (CISO) and that specify how an agency's information security manager must interact with the agency CISO.

COMMITTEE/SUBCOMMITTEE ACTION

ADOPTED	__ (Y/N)
ADOPTED AS AMENDED	__ (Y/N)
ADOPTED W/O OBJECTION	__ (Y/N)
FAILED TO ADOPT	__ (Y/N)
WITHDRAWN	__ (Y/N)
OTHER	_____

Committee/Subcommittee hearing bill: Energy, Communications & Cybersecurity Subcommittee
Representative Giallombardo offered the following:

Amendment (with title amendment)
Remove lines 90-100

T I T L E A M E N D M E N T

Remove lines 2-5 and insert:
An act relating to cybersecurity; amending s. 282.0041,

COMMITTEE/SUBCOMMITTEE ACTION

ADOPTED	__ (Y/N)
ADOPTED AS AMENDED	__ (Y/N)
ADOPTED W/O OBJECTION	__ (Y/N)
FAILED TO ADOPT	__ (Y/N)
WITHDRAWN	__ (Y/N)
OTHER	_____

Committee/Subcommittee hearing bill: Energy, Communications & Cybersecurity Subcommittee
Representative Giallombardo offered the following:

Amendment (with title amendment)

Remove lines 611-635 and insert:

(a) Designate an information security manager to ensure compliance with cybersecurity governance and with the state's enterprise security program and incident response plan. The information security manager must coordinate with the agency's information security personnel and the Cybersecurity Operations Center to ensure that the unique needs of the agency are met ~~administer the cybersecurity program of the state agency~~. This designation must be provided annually in writing to the department by January 15 ~~1~~. A state agency's information

security manager, for purposes of these information security duties, shall report directly to the agency head.

T I T L E A M E N D M E N T

Remove lines 53-55 and insert:
certain measures; revising the purpose of

HB 7047

HOUSE OF REPRESENTATIVES STAFF ANALYSIS

BILL #: HB 7047 PCB EEG 24-07 OGSR/Utility Owned or Operated by a Unit of Local Government
SPONSOR(S): Ethics, Elections & Open Government Subcommittee, Porras
TIED BILLS: **IDEN./SIM. BILLS:** SB 7006

REFERENCE	ACTION	ANALYST	STAFF DIRECTOR or BUDGET/POLICY CHIEF
Orig. Comm.: Ethics, Elections & Open Government Subcommittee	16 Y, 0 N	Poreda	Toliver
1) Energy, Communications & Cybersecurity Subcommittee		Phelps	Keating
2) State Affairs Committee			

SUMMARY ANALYSIS

The Open Government Sunset Review (OGSR) Act requires the Legislature to review each public record exemption and each public meeting exemption five years after enactment. If the Legislature does not reenact the exemption, it automatically repeals on October 2nd of the fifth year after enactment.

Municipalities are authorized by general law to provide water and sewer utility services, as well as electric and natural gas utility services. Counties are authorized to provide water and sewer utility services both within their individual boundaries and in adjoining counties. Current law provides public record exemptions for the following information held by a utility owned or operated by a unit of local government (local government utility):

- Information related to the security of a local government utility's technology, processes, and practices designed to protect the utility's networks, computers, programs, and data from attack, damage, or unauthorized access that, if disclosed, would facilitate the alteration, disclosure, or destruction of such data or information technology (I.T.) resources.
- Information related to the security of a local government utility's existing or proposed I.T. systems or industrial control technology systems that, if disclosed, would facilitate unauthorized access to, and alteration or destruction of, such systems in a manner that would adversely impact the safe and reliable operations of the systems and the utility.
- Customer meter-derived data and billing information in increments of less than one billing cycle.

Current law also provides a public meeting exemption for the portions of meetings held by a local government utility that would reveal information exempt from disclosure by the public records exemptions discussed above. The exemption requires that all closed portions be recorded and transcribed and that such recordings and transcripts are confidential and exempt from disclosure as public records.

In 2022, the Legislature created a general public record exemption, applicable to all agencies, for certain information related to cybersecurity. Pursuant to the OGSR Act, the exemption for cybersecurity information will repeal on October 2, 2027, unless reviewed and saved from repeal by the Legislature.

The bill extends the repeal date for the public record exemptions related to I.T. security and the public meeting exemption to October 2, 2027, to coincide with the future OGSR repeal date of the general cybersecurity exemption in statute. The bill saves from repeal the public record exemption related to customer meter-derived data and billing information. Each of the exemptions will repeal on October 2, 2024, if this bill does not become law.

The bill does not appear to have a fiscal impact on state government or local governments.

FULL ANALYSIS

I. SUBSTANTIVE ANALYSIS

A. EFFECT OF PROPOSED CHANGES:

Background

Open Government Sunset Review Act

The Open Government Sunset Review Act (OGSR Act)[1] sets forth a legislative review process for newly created or substantially amended public record or public meeting exemptions. It requires an automatic repeal of the exemption on October 2nd of the fifth year after creation or substantial amendment, unless the Legislature reenacts the exemption.[2]

The OGSR Act provides that a public record or 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 effectively and efficiently 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.[3]

If, and only if, in reenacting an exemption that will repeal, the exemption is expanded, then a public necessity statement and a two-thirds vote for passage are required. If the exemption is reenacted with grammatical or stylistic changes that do not expand the exemption, if the exemption is narrowed, or if an exception to the exemption is created, then a public necessity statement and a two-thirds vote are not required.[4]

Local Government Utilities

The Florida Constitution grants municipalities the governmental, corporate, and proprietary powers necessary to enable them to conduct municipal government, perform municipal functions, and render municipal services, and permits them to exercise any power for municipal purposes, except when expressly prohibited by law.[5]

Counties not operating under a charter have the power of self-government as provided by general or special law, while charter counties have all powers of self-government not inconsistent with general law or with special law approved by the county electors.[6] Counties are authorized by general law to provide water and sewer utility services both within their individual boundaries and in adjoining counties.[7] Municipalities are authorized by general law to provide water and sewer utility services[8] as well natural gas services[9] and electric and gas utilities[10]

Florida Public Service Commission

[1] S. 119.15, F.S.
[2] S. 119.15(3), F.S.
[3] S. 119.15(6)(b), F.S.
[4] Article I, s. 24(c), Fla. Const.
[5] Article VIII, s. 2(b), Fla. Const.
[6] Article VIII, s. 1(f)-(g), Fla. Const.
[7] Ss. 125.01(1)(k)1., F.S. and 153.03, F.S.
[8] Pursuant to s. 180.06, F.S., a municipality may "provide water and alternative water supplies;" "provide for the collection and disposal of sewage, including wastewater reuse, and other liquid wastes;" and "construct reservoirs, sewerage systems, trunk sewers, intercepting sewers, pumping stations, wells, siphons, intakes, pipelines, distribution systems, purification works, collection systems, treatment and disposal works" to accomplish these purposes.
[9] S. 180.06(8), F.S.
[10] Ch. 366, F.S.

The Florida Public Service Commission (PSC) ensures Florida's consumers receive utility services, including electric, natural gas, telephone, water, and wastewater, "in a safe, affordable, and reliable manner."[11] The PSC primarily regulates investor owned utilities but is able to exercise limited authority over publicly owned utilities in the following areas:[12]

- Rate base or economic regulation.
- Competitive market oversight.
- Monitoring of safety, reliability and service.

Utility Customer Consumption Data

Traditional, analog utility meters record consumption at a utility customer's premises. On a regular, periodic basis, the meter is "read" in person by a utility employee to determine how much of the utility's service — electric, natural gas, or water/wastewater — was used at the premises since the last meter reading. This data is used by the utility for purposes of customer billing. In recent years, utilities have deployed, to varying degrees, newer "smart meter"[13] technologies that measure a utility customer's consumption on a more frequent basis (e.g., hourly) and transmit this data automatically and wirelessly to the utility. The utility still uses this data for billing purposes but can also use it to monitor its system and identify and locate problems more quickly.[14]

Cybersecurity Public Record Exemption

In 2022, the Legislature passed CS/HB 7057, which created a general public record exemption — applicable to all agencies[15] — for the certain information related to cybersecurity.[16] Specifically, CS/HB 7057, which was codified as s. 119.0725, F.S., protected the following information:

- Information related to critical infrastructure.[17]
- 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, 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
    - Information technology (I.T.) resources, which include an agency's existing or proposed I.T. systems.
- Coverage limits and deductible or self-insurance amounts of insurance or other risk mitigation coverages acquired for the protection of I.T. systems, operational technology systems, or data of an agency.
- Cybersecurity incident information contained in certain reports.

CS/HB 7057 (2022) also created a public meeting exemption for any portion of a meeting that would reveal the confidential and exempt information; however, any portion of an exempt meeting must be recorded and transcribed.[18] The recording and transcript are confidential and exempt from public record requirements.[19]

[11] Florida Public Service Commission, *About*, *available at* https://www.psc.state.fl.us/about (last visited Jan. 15, 2024).
[12] Florida Public Service Commission, *2022 Annual Report*, *available at* https://www.floridapsc.com/pscfiles/website-files/PDF/Publications/Reports/General/AnnualReports/2022.pdf (last visited January 16, 2024)
[13] *See* Florida Public Service Commission, *Smart Meters*, *available at* https://www.floridapsc.com/pscfiles/website-files/pdf/Utilities/Electricgas/SmartMeters/SmartMeter.pdf (last visited January 16, 2024).
[14] *Id.*
[15] "Agency" means 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 ch. 119, F.S., 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. S. 119.011(2), F.S.
[16] *See* s. 119.0725, F.S.
[17] "Critical infrastructure" means existing and proposed information technology and operation technology systems and assets, whether physical and virtual, the incapacity or destruction of which would negatively affect security, economic security, public health, or public safety. S. 119.0725(1)(b), F.S.
[18] S. 119.0725(3), F.S.
[19] *Id.*

Public Record and Public Meeting Exemptions under Review

In 2016, the Legislature created a public record exemption that made the following information held by a utility[20] owned or operated by a unit of local government (local government utility) confidential and exempt[21] from public record requirements:

- Information related to the security of a local government utility's technology, processes, and practices designed to protect the utility's networks, computers, programs, and data from attack, damage, or unauthorized access that, if disclosed, would facilitate the alteration, disclosure, or destruction of such data or I.T. resources.
- Information related to the security of a local government utility's existing or proposed I.T. systems or industrial control technology systems that, if disclosed, would facilitate unauthorized access to, and alteration or destruction of, such systems in a manner that would adversely impact the safe and reliable operations of the systems and the utility.[22]

In 2019, the Legislature created a public record exemption that made customer meter-derived data and billing information in increments of less than one billing cycle held by a local government utility confidential and exempt from public record requirements.[23] Additionally, in that same year, the Legislature created a public meeting exemption for any portion of a meeting held by a local government utility that would reveal information made exempt pursuant to the local government utility's public record exemption.[24] All closed portions of such a meeting must be recorded and transcribed and such recording or transcription are exempt from public record requirements.[25]

The 2016 public necessity statement[26] for the public record exemptions for certain I.T. security information provided that:

> [M]any utilities have adopted technologies, processes, and practices designed to secure data, information technology systems, and industrial control technology systems. Disclosure of sensitive information related to these security measures could result in the identification of vulnerabilities that allow a security breach that damages utility systems and disrupts the safe and reliable operation of such systems, adversely impacting the public health and safety and the economic well-being of the state. Because of the interconnected nature of utility systems, a security breach may also impact national security concerns.[27]

The 2019 public necessity statement for the public record exemption for customer meter-derived data and billing information provided that:

> Smart meters, which can record and transmit detailed data on a customer's use of utility services, present unique security concerns. These concerns were addressed in a report released in October 2010 by the United States Department of Energy titled "Data Access and Privacy Issues related to Smart Grid Technologies." The

[20] "Utility" means a person or entity that provides electricity, natural gas, telecommunications, water, chilled water, reuse water, or wastewater. S. 119.011(15), F.S.

[21] There is a difference between records the Legislature designates *exempt* from public record requirements and those the Legislature designates *confidential and exempt*. A record classified as exempt from public disclosure may be disclosed under certain circumstances. *See WFTV, Inc. v. Sch. Bd. of Seminole*, 874 So.2d 48, 53 (Fla. 5th DCA 2004), *review denied*, 892 So.2d 1015 (Fla. 2004); *State v. Wooten*, 260 So. 3d 1060, 1070 (Fla. 4th DCA 2018); *City of Rivera Beach v. Barfield*, 642 So.2d 1135 (Fla. 4th DCA 1994); *Williams v. City of Minneola*, 575 So.2d 683, 687 (Fla. 5th DCA 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* Op. Att'y Gen. Fla. 04-09 (2004).

[22] Chapter 2016-95, L.O.F., codified as s. 119.0713(5), F.S.

[23] Chapter 2019-38, LO.F., codified as s. 119.0713(5)(a)3., F.S.

[24] Chapter 2019-37, L.O.F., codified as s. 286.0113(3), F.S.

[25] S. 286.0113(3)(a), F.S. However, a court of competent jurisdiction, following an in-camera review, may determine that the meeting was not restricted to the discussion of data and information made exempt, and in that event, the portion of the recording or transcript which reveals nonexempt data and information may be disclosed to a third party.

[26] Article I, s. 24(c), FLA. CONST., requires each public record exemption to "state with specificity the public necessity justifying the exemption."

[27] Ch. 2016-95, L.O.F.

> report recommended that customer data be protected from release to third parties. This detailed customer data can be used to specifically identify minute-by-minute usage patterns, including the exact appliance or service being used. This information creates significant security issues for both businesses and homeowners.[28]

The 2019 public necessity statement for the public meeting exemption provided that:

> [A]s utility system infrastructure becomes more connected and integrated through information and communications technology, the exposure to damage from attacks through such technology grows. These attacks may result in the disruption of utility services and damage to utility systems. Maintaining safe and reliable utility systems is vital to protecting the public health and safety and to ensuring the economic well-being of this state.[29]

Pursuant to the OGSR Act, each of the above exemptions will repeal on October 2, 2024, unless reenacted by the Legislature.

During the 2023 interim, House and Senate committee staff jointly developed a questionnaire and sent the questionnaires to city and county governments. In total, staff received 39 responses from those entities.[30] Most respondents indicated that they were unaware of any litigation concerning the exemptions and had not encountered any issues interpreting or applying the exemptions. The vast majority of respondents indicated that the exemptions be reenacted as is and no respondent recommended eliminating the public record or public meeting exemptions. As a part of the questionnaire, respondents were asked to consider whether the local government utility I.T. security exemptions were duplicative of the general cybersecurity exemption in s. 119.0725, F.S. Some respondents noted that there may be some overlap between the exemption.

Effect of the Bill

The bill extends the repeal date for the public record exemptions related to local government utility I.T. security and the public meeting exemption to October 2, 2027, to coincide with the future OGSR repeal date of the general cybersecurity exemption in s. 119.0725, F.S. The bill saves from repeal the public record exemption for customer meter-derived data and billing information in increments of less than one billing cycle held by a local government utility. Each of the exemptions under review will repeal on October 2, 2024, if this bill does not become law

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 amends s. 286.0113, F.S., relating to general exemptions from public meetings.

Section 3 provides an effective date of October 1, 2024.

II. FISCAL ANALYSIS & ECONOMIC IMPACT STATEMENT

A. FISCAL IMPACT ON STATE GOVERNMENT:

1. Revenues:

None.

[28] Ch. 2019-38, L.O.F.
[29] Ch. 2019-37, L.O.F.
[30] Open Government Sunset Review Questionnaire, Public Records and Public Meetings Related to utilities owned or operated by a unit of local government, responses on file with the Ethics, Elections & Open Government Subcommittee.

2. Expenditures:

None.

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. The 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 and municipalities have to raise revenues in the aggregate; or reduce the percentage of state tax shared with counties and municipalities.

2. Other:

None.

B. RULE-MAKING AUTHORITY:

The bill does not require rulemaking nor confer rulemaking authority.

C. DRAFTING ISSUES OR OTHER COMMENTS:

None.

IV. AMENDMENTS/COMMITTEE SUBSTITUTE CHANGES

Not applicable.

A bill to be entitled

An act relating to a review under the Open Government Sunset Review Act; amending s. 119.0713, F.S., which provides exemptions from public records requirements for information related to the security of certain technology, processes, practices, information technology systems, and industrial control technology systems and certain customer meter-derived data and billing information held by a utility owned or operated by a unit of local government; extending the date of scheduled repeal of the public records exemptions for such information; removing the scheduled repeal of the public records exemption for such customer meter-derived data and billing information; amending s. 286.0113, F.S., which provides an exemption from public meetings requirements for portions of meetings held by a utility owned or operated by a unit of local government that would reveal certain information; extending the date of scheduled repeal of the public meetings exemption; providing an effective date.

Be It Enacted by the Legislature of the State of Florida:

Section 1. Subsection (5) of section 119.0713, Florida

CODING: Words ~~stricken~~ are deletions; words underlined are additions.

Statutes, is amended to read:

119.0713 Local government agency exemptions from inspection or copying of public records.—

(5)(a) The following information held by a utility owned or operated by a unit of local government is exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution:

1. Information related to the security of the technology, processes, or practices of a utility owned or operated by a unit of local government that are designed to protect the utility's networks, computers, programs, and data from attack, damage, or unauthorized access, which information, if disclosed, would facilitate the alteration, disclosure, or destruction of such data or information technology resources.

2. Information related to the security of existing or proposed information technology systems or industrial control technology systems of a utility owned or operated by a unit of local government, which, if disclosed, would facilitate unauthorized access to, and alteration or destruction of, such systems in a manner that would adversely impact the safe and reliable operation of the systems and the utility.

3. Customer meter-derived data and billing information in increments less than one billing cycle.

(b) This exemption applies to such information held by a utility owned or operated by a unit of local government before, on, or after the effective date of this exemption.

(c) Subparagraphs (a)1. and 2. are ~~This subsection is~~ subject to the Open Government Sunset Review Act in accordance with s. 119.15 and shall stand repealed on October 2, 2027 ~~2024~~, unless reviewed and saved from repeal through reenactment by the Legislature.

Section 2. Subsection (3) of section 286.0113, Florida Statutes, is amended to read:

286.0113 General exemptions from public meetings.—

(3)(a) That portion of a meeting held by a utility owned or operated by a unit of local government which would reveal information that is exempt under s. 119.0713(5) is exempt from s. 286.011 and s. 24(b), Art. I of the State Constitution. All exempt portions of such a meeting must be recorded and transcribed. The recording and transcript of the meeting are exempt from disclosure under s. 119.07(1) and s. 24(a), Art. I of the State Constitution unless a court of competent jurisdiction, following an in camera review, determines that the meeting was not restricted to the discussion of data and information made exempt by this section. In the event of such a judicial determination, only the portion of the recording or transcript which reveals nonexempt data and information may be disclosed to a third party.

(b) This subsection is subject to the Open Government Sunset Review Act in accordance with s. 119.15 and shall stand repealed on October 2, 2027 ~~2024~~, unless reviewed and saved from

repeal through reenactment by the Legislature.

Section 3. This act shall take effect October 1, 2024.