HOUSE OF REPRESENTATIVES STAFF ANALYSIS

BILL #: CS/HB 7055 PCB SAT 22-02 Cybersecurity
SPONSOR(S): State Affairs Committee, State Administration & Technology Appropriations Subcommittee, Giallombardo, Fischer and others
TIED BILLS: CS/HB 7057 **IDEN./SIM. BILLS:** CS/SB 1670

REFERENCE	ACTION	ANALYST	STAFF DIRECTOR or BUDGET/POLICY CHIEF
Orig. Comm.: State Administration & Technology Appropriations Subcommittee	14 Y, 0 N	Mullins	Topp
1) State Affairs Committee	23 Y, 0 N, As CS	Villa	Williamson

SUMMARY ANALYSIS

The State Cybersecurity Act requires the Florida Digital Service (FLDS) and the heads of state agencies to meet certain requirements to enhance the cybersecurity of state agencies. Currently, state agencies must provide cybersecurity training to their employees, report cybersecurity incidents, and adopt cybersecurity standards. However, there are no such requirements for counties and municipalities (local governments).

Current law regarding state or local government cybersecurity does not specifically address ransomware, which is a form of malware designed to encrypt files on a device, rendering any files unusable. Malicious actors then demand ransom in exchange for decryption.

The bill prohibits state agencies and local governments from paying or otherwise complying with a ransomware incident.

The bill defines the severity level of a cybersecurity incident in accordance with the National Cyber Incident Response Plan. State agencies and local governments must report all ransomware incidents and high severity level cybersecurity incidents to the Cybersecurity Operations Center (CSOC) and the Cybercrime Office within the Florida Department of Law Enforcement as soon as possible but no later than a time certain. Local governments must also report to the sheriff. The bill requires state agencies to report low level cybersecurity incidents and provides that local governments may report such incidents. The bill also requires state agencies and local governments to submit after-action reports to FLDS following a cybersecurity or ransomware incident.

The bill requires the CSOC to notify the Legislature of high severity level cybersecurity incidents. The notice must contain a high-level overview of the incident and its likely effects. In addition, the CSOC must provide the Legislature and the Cybersecurity Advisory Council (CAC) with a consolidated incident report on a quarterly basis.

The bill requires state agency and local government employees to undergo certain cybersecurity training within 30 days of employment and annually thereafter.

The bill requires local governments to adopt cybersecurity standards that safeguard the local government's data, information technology (IT), and IT resources.

The bill expands the purpose of the CAC to include advising local governments on cybersecurity and requires the CAC to examine reported cybersecurity and ransomware incidents to develop best practice recommendations. The CAC must submit an annual comprehensive report regarding ransomware to the Governor and Legislature.

The bill establishes penalties and fines for certain ransomware offenses against a government entity.

The bill will likely have a negative fiscal impact on state and local government expenditures; however, the bill may also have a positive fiscal impact on the state due to the punitive fine established in the bill. *See* Fiscal Analysis & Economic Impact Statement.

FULL ANALYSIS

I. SUBSTANTIVE ANALYSIS

A. EFFECT OF PROPOSED CHANGES:

Background

Ransomware

Ransomware is a form of malware[1] designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. Ransomware actors often target and threaten to sell or leak exfiltrated data or authentication information if the ransom is not paid. In recent years, ransomware incidents have become increasingly prevalent among the nation's state, local, tribal, and territorial government entities and critical infrastructure organizations.[2] In 2021, state chief information officers overwhelmingly named ransomware as their top cybersecurity concern.[3]

While most ransomware attacks are not reported in the news, in 2021 at least 2,323 state and local governments, schools, and healthcare providers experienced ransomware attacks.[4] Ransomware attacks on such entities have resulted in medical records being inaccessible or permanently lost; surgical procedures being canceled, tests postponed, and admissions halted; schools closing; students' grades being lost; 911 services interrupted; police being locked out of background check systems; surveillance systems going offline; badge scanners and building access systems ceasing to work; property transactions being halted; websites going offline; online payment portals being inaccessible; email and phone systems ceasing to work; driver licenses not being issued or renewed; and payments to vendors being delayed.

National Institute for Standards and Technology Cybersecurity Framework

The National Institute for Standards and Technology (NIST) is a non-regulatory federal agency housed within the United States Department of Commerce. NIST is charged with providing a prioritized, flexible, repeatable, performance-based, and cost-effective framework that helps owners and operators of critical infrastructure identify, assess, and manage cyber risk. While the framework was developed with critical infrastructure in mind, it can be used by organizations in any sector of the economy or society.[5] The framework is designed to complement, and not replace, an organization's own unique approach to cybersecurity risk management. As such, there are a variety of ways to use the framework and the decision about how to apply it is left to the implementing organization. For example, an organization may use its current processes and consider the framework to identify opportunities to strengthen its cybersecurity risk management. Overall, the framework provides an outline of best practices that helps organizations decide where to focus resources for cybersecurity protection.[6]

---

[1] "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 January 30, 2022).

[2] Cybersecurity and Infrastructure Agency, *Ransomware 101,* https://www.cisa.gov/stopransomware/ransomware-101 (last visited January 30, 2022).

[3] National Association of State Chief Information Officers, *Driving digital acceleration The 2021 State CIO Survey* (October 2021), *available at* https://www.nascio.org/wp-content/uploads/2021/10/2021-State-CIO-Survey.pdf (last visited January 30, 2022).

[4] Emsisoft Malware Lab, *The State of Ransomware in the US: Report and Statistics 2021* (January 18, 2022), *available at* https://blog.emsisoft.com/en/40813/the-state-of-ransomware-in-the-us-report-and-statistics-2021/ (last visited January 30, 2022). These numbers do not include ransomware attacks that were reported in the press as cyberattacks or attacks on third party service and solution providers.

[5] National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity, *available at* https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (last visited January 30, 2022).

[6] *Id*.

National Cyber Incident Response Plan

The National Cyber Incident Response Plan (NCIRP) was developed according to the direction of Presidential Policy Directive (PPD)-41,[7] 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.[8] The NCIRP is not a tactical or operational plan; rather, it serves as the primary strategic framework for stakeholders to understand how federal departments and agencies and other national-level partners provide resources to support response operations. 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 common 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.[9]

Figure 1: Cybersecurity Incident Severity Schema

Disaster Level	Cyber Incident Severity	Description
Level 1	Level 5 *Emergency*	Poses an imminent threat to the provision of wide-scale critical infrastructure services, national government security, or the lives of US citizens.
Level 2	Level 4 *Severe*	Likely to result in a significant impact to public health or safety, national security, economic security, foreign relations, or civil liberties.
	Level 3 *High*	Likely to result in a demonstrable impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
Level 3	Level 2 *Medium*	May impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
	Level 1 *Low*	Unlikely to impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.

[7] 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 February 18, 2022).
[8] U.S. Department of Homeland Security, *National Cyber Incident Response Plan* (December 2016) available at: file:///C:/Users/Villa.Chris/Downloads/798128%20(7).pdf (last visited February 20, 2022).
[9] *Id*.

Information Technology Management

The Department of Management Services (DMS)[10] oversees information technology (IT)[11] governance and security for the executive branch of state government. The Florida Digital Service (FLDS) within DMS was established by the Legislature in 2020 to replace the Division of State Technology.[12] The head of FLDS is appointed by the Secretary of Management Services[13] and serves as the state chief information officer (CIO).[14]

FLDS was created to 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.[15] Accordingly, 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[16] must comply when implementing IT projects.
- Perform project oversight on 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.[17]
- 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.[18]

State Cybersecurity Act

The State Cybersecurity Act[19] requires DMS and the heads of state agencies[20] to meet certain requirements to enhance the cybersecurity[21] of state agencies. Specifically, DMS, acting through FLDS must:

- Establish standards and processes for assessing state agency cybersecurity risks and determining appropriate security measures consistent with generally accepted best practices for cybersecurity, including the NIST cybersecurity framework.
- Adopt rules to mitigate risk, support a security governance framework, and safeguard state agency digital assets, data,[22] information, and IT resources[23] to ensure availability, confidentiality, and integrity.

---

[10] *See* s. 20.22, F.S.

[11] 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. Section 282.0041(20), F.S.

[12] Ch. 2020-161, L.O.F.

[13] The Secretary of Management Services serves as the head of DMS and is appointed by the Governor, subject to confirmation by the Senate. Section 20.22(1), F.S.

[14] Section 282.0051(2)(a), F.S.

[15] Section 282.0051(1), F.S.

[16] "State agency" means any official, officer, commission, board, authority, council, committee, or department of the executive branch of state government; the Justice Administrative Commission; and the Public Service Commission. The term does not include university boards of trustees, state universities, the Department of Legal Affairs, the Department of Agriculture and Consumer Services, or the Department of Financial Services. Section 282.0041(33), F.S.

[17] For the Department of Financial Services, the Department of Legal Affairs, and the Department of Agriculture and Consumer Services, FDS provides project oversight on IT projects that have a total cost of $20 million or more. Section 282.0051(1)(n), F.S.

[18] Section 282.0051(1), F.S.

[19] Section 282.318, F.S.

[20] 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. Section 282.318(2), F.S.

[21] "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 information technology resources. Section 282.0041(8), F.S.

[22] "Data" means a subset of structured information in a format that allows such information to be electronically retrieved and transmitted. Section 282.0041(9), F.S.

[23] "Information technology resources" means data processing hardware and software and services, communications, supplies, personnel, facility resources, maintenance, and training. Section 282.0041(22), F.S.

- Designate a chief information security officer (CISO) responsible for the development, operation, and oversight of cybersecurity for state technology systems. The CISO must be notified of all confirmed or suspected incidents or threats of state agency IT resources and must report such information to the CIO and the Governor.
- Develop and annually update 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 cyber incidents.[24]
- Develop and publish for use by state agencies a cybersecurity governance framework.
- Assist state agencies in complying with the State Cybersecurity Act.
- In collaboration with the Cybercrime Office within the Florida Department of Law Enforcement (FDLE), 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.
- Annually review the strategic and operational cybersecurity plans of state agencies.
- Track, in coordination with agency inspectors general, state agencies' implementation of remediation plans.
- Provide cybersecurity training to all state agency technology professionals that develops, assesses, and documents competencies by role and skill level. The training may be provided in collaboration with the Cybercrime Office, a private sector entity, or an institution of the state university system.
- Operate and maintain a Cybersecurity Operations Center led by the CISO to serve as a clearinghouse for threat information and to coordinate with FDLE to support state agency response to cybersecurity incidents.
- Lead an Emergency Support Function under the state comprehensive emergency management plan.[25]

The State Cybersecurity Act requires the head of each state agency to designate an information security manager to administer the cybersecurity program of the state agency.[26] In addition, the head of each state agency must:

- Establish an agency cybersecurity incident response team in consultation with FLDS and the Cybercrime Office. The agency cybersecurity incident response team must convene upon notification of a cybersecurity incident and 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 every three years a comprehensive risk assessment to determine the security threats to the data, information, and IT resources of the state agency.
- Develop and periodically update written internal policies and procedures, including procedures for reporting cybersecurity incidents and breaches to FLDS and the Cybercrime Office.
- Implement managerial, operational, and technical safeguards and risk assessment remediation plans recommended by DMS to address identified risks to the data, information, and IT resources of the agency.
- Ensure that periodic internal audits and evaluations of the agency's cybersecurity program for the data, information, and IT resources of the agency are conducted.
- Ensure that the cybersecurity requirements in written specifications for the solicitation, contracts, and service-level agreement of IT and IT resources and services meet or exceed applicable state and federal laws, regulations, and standards for cybersecurity, including the NIST cybersecurity framework.
- Provide cybersecurity awareness training to all state agency employees within 30 days of commencing employment concerning cybersecurity risks and the responsibility of employees to comply with policies, standards, guidelines, and operating procedures adopted by the state

[24] "Incident" means a violation or imminent threat of violation, whether such violation is accidental or deliberate, of information technology 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. Section 282.0041(19), F.S.

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

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

agency to reduce those risks. The training may be provided in collaboration with the Cybercrime Office, a private sector entity, or an institution of the state university system.
- 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 (CAC) within DMS[28] assists state agencies in protecting IT resources from cyber threats and incidents.[29] 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.[30] 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 for state agencies, including continuous risk monitoring, password management, and protecting data in legacy and new systems.
- Examine inconsistencies between state and federal law regarding cybersecurity.[31]

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.[32]

Beginning June 30, 2022, and each June 30 thereafter, the CAC must submit to the Legislature any recommendations considered necessary by the CAC to address cybersecurity.[33]

Offenses against Users of Computers

Florida law criminalizes the following acts involving a computer,[34] computer system,[35] computer network,[36] or electronic device[37] when done knowingly, willfully, and without authorization:
- Accessing[38] or causing to be accessed any computer, computer system, computer network, or electronic device with knowledge that such access is unauthorized or the manner or use exceeds authorization.
- Disrupting or denying the ability to transmit data to or from an authorized user of a computer, computer system, computer network, or electronic device under certain circumstances.

[27] Section 282.318(4), F.S.
[28] Section 282.319(1), F.S.
[29] Section 282.319(2), F.S.
[30] Section 282.319(3), F.S.
[31] Section 282.319(9), F.S.
[32] Section 282.319(10), F.S.
[33] Section 282.319(11), F.S.
[34] "Computer" means an internally programmed, automatic device that performs data processing. Section 815.03(2), F.S.
[35] "Computer system" means a device or collection of devices, including support devices, one or more of which contain computer programs, electronic instructions, or input data and output data, and which perform functions, including, but not limited to, logic, arithmetic, data storage, retrieval, communication, or control. The term does not include calculators that are not programmable and that are not capable of being used in conjunction with external files. Section 815.03(7), F.S.
[36] "Computer network" means a system that provides a medium for communication between one or more computer systems or electronic devices, including communication with an input or output device such as a display terminal, printer, or other electronic equipment that is connected to the computer systems or electronic devices by physical or wireless telecommunication facilities. Section 815.03(4), F.S.
[37] "Electronic device" means a device or a portion of a device that is designed for and capable of communicating across a computer network with other computers or devices for the purpose of transmitting, receiving, or storing data, including, but not limited to, a cellular telephone, tablet, or other portable device designed for and capable of communicating with or across a computer network and that is actually used for such purpose. Section 815.03(9), F.S.
[38] "Accessing" means approaching, instructing, communicating with, storing data in, retrieving data from, or otherwise making use of any resources of a computer, computer system, computer network, or electronic device. Section 815.03(1), F.S.

- Destroying, taking, injuring, or damaging computers, computer systems, computer networks, or electronic devices.
- Introducing a computer contaminant into a computer, computer system, computer network, or electronic device.
- Engaging in audio or video surveillance of an individual by accessing one of the inherent features or components of a computer, computer system, computer network, or electronic device, including accessing the data or information stored by a third party.[39]

In general, such conduct against a computer user is a third degree felony,[40] punishable by up to five years in prison and a $5,000 fine.[41] However, the crime may be enhanced to a second[42] or first[43] degree felony with aggravating factors, such as excessive damage or endangering a human life.[44]

Effect of the Bill

Ransomware Incident

The bill defines "ransomware incident" to mean a malicious cybersecurity incident in which a person or entity introduces software that gains unauthorized access to or encrypts, modifies, or otherwise renders unavailable a state agency's or local government's[45] data and thereafter the person or entity demands a ransom to restore access to the data, prevent publication of the data, or otherwise remediate the impact of the software. The bill prohibits a state agency or local government experiencing a ransomware incident from paying or otherwise complying with the demanded ransom.

Cybersecurity and Ransomware Incident Notification

The bill defines the severity level of a cybersecurity incident in accordance with the NCIRP 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.
- 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.

The bill requires state agencies and local governments to report all ransomware incidents as soon as possible, but no later than 12 hours after discovery of the incident. It also requires state agencies and local governments to report cybersecurity incidents determined to be of severity level three, four, or five as soon as possible, but no later than 48 hours after discovery of the incident. Local governments may report cybersecurity incidents determined to be of severity level one or two and state agencies are required to report such incidents as soon as possible. State agencies and local governments report the incidents to the CSOC and Cybercrime Office; however, local governments are also required to report to the sheriff that has jurisdiction over the local government.

The bill specifies the information that must be reported in a cybersecurity or ransomware incident report by a state agency or local government. The incident report must include, at a minimum:

[39] Section 815.06(2), F.S.
[40] Section 815.06(3)(a), F.S.
[41] Section 775.082 and 775.083, F.S.
[42] A second degree felony is punishable by up to 15 years in prison and a $10,000 fine. Sections 775.082 and 775.083, F.S.
[43] A first degree felony is punishable by up to 30 years in prison and a $10,000 fine. Sections 775.082 and 775.083, F.S.
[44] Section 815.06(3)(b) and (3)(c), F.S.
[45] The bill defines "local government" to mean a county or a municipality.

- 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.
- If the reporting entity is a local government, a statement requesting or declining assistance from the CSOC, Cybercrime Office, or sheriff.

The bill requires the CSOC to notify the President of the Senate and the Speaker of the House of Representatives of any cybersecurity incident with a severity level of three, four, or five within 12 hours of receiving the state agency or local government incident report. The notification must include a high-level description of the incident and the likely effects. In addition, the CSOC must provide consolidated incident reports to the President of the Senate, Speaker of the House of Representatives, and CAC on a quarterly basis. 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.

After-action Reports

The bill requires state agencies and local governments to submit an after-action report to FLDS within one week of the remediation of a cybersecurity or ransomware incident. The after-action report must summarize the incident, the incident's resolution, and any insights gained as a result of the incident. By December 1, 2022, FLDS must establish guidelines and processes for submitting after-action reports.

Cybersecurity Training

The bill requires FLDS to develop a basic and advanced cybersecurity training curriculum. All local government employees with access to the local government's network must complete the basic training curriculum, and local government technology professionals and employees with access to highly sensitive information must complete the advanced training curriculum. The trainings must be completed by employees within 30 days of commencing employment and on an annual basis thereafter. The bill authorizes FLDS to provide the cybersecurity trainings in collaboration with the Cybercrime Office, a private sector entity, or an institution of the State University System.

The bill requires the advanced cybersecurity training currently provided by FLDS to state agency technology professionals to be provided on an annual basis and to be provided to employees with access to highly sensitive information. In addition, state agency heads must provide the basic cybersecurity training that is currently provided to agency employees on an annual basis.

The bill requires the advanced cybersecurity training curriculum provided to certain state and local government employees to include training on the identification of each cybersecurity incident severity level.

Local Government Cybersecurity Standards

The bill requires local governments to adopt cybersecurity standards that safeguard the local government's data, IT, and IT resources to ensure availability, confidentiality, and integrity. The standards must be consistent with generally accepted best practices for cybersecurity, including the NIST cybersecurity framework. Counties with a population of 75,000 or more and municipalities with a population of 25,000 or more must adopt the standards by January 1, 2024. Counties with a population less than 75,000 and municipalities with a population less than 25,000 must adopt the standards by January 1, 2025. The bill requires each local government to notify FLDS when it has adopted the standards.

Florida Cybersecurity Advisory Council

The bill provides that one of the purposes of the CAC is to advise local governments on cybersecurity, including cybersecurity threats, trends, and best practices. In addition, the bill requires the CAC to review information relating to cybersecurity and ransomware incidents reported by state agencies and

local governments to determine commonalities and develop best practice recommendations for those entities. The CAC must recommend any additional information that should be reported by a local government to FLDS as part of a cybersecurity or ransomware incident report.

Beginning December 1, 2022, and each December 1 thereafter, the CAC must 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. At a minimum, the report must include:

- 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 lead 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.
- Other recommendations to prevent ransomware incidents.

The bill specifies that, for purposes of the CAC's charter, the term "state agency" includes the Department of Legal Affairs, the Department of Agriculture and Consumer Services, and the Department of Financial Services.

Ransomware Offense

The bill provides that a person who willfully, knowingly, and without authorization introduces a computer contaminant that gains unauthorized access to, encrypts, modifies, or otherwise renders unavailable data, programs, or supporting documentation residing or existing within a computer, computer system, computer network, or electronic device owned or operated by a government entity[46] and demands a ransom to prevent the publication of or restore access to the data, programs, or supporting documentation or to otherwise remediate the impact of the computer contaminant commits a ransomware offense. The bill provides that a ransomware offense is punishable as a first degree felony. The bill further provides that an employee or contractor of a government entity, with access to the government entity's network, who willfully and knowingly aids or abets another in the commission of a ransomware offense against the government entity commits a felony of the first degree. In addition to any other penalties imposed, the convicted person must pay a fine equal to twice the amount demanded in the ransomware offense, the proceeds of which will be deposited into the General Revenue Fund.

B. SECTION DIRECTORY:

Section 1 amends s. 282.0041, F.S., relating to definitions.

Section 2 amends s. 282.318, F.S., relating to cybersecurity.

Section 3 creates s. 282.3185, F.S., relating to local government cybersecurity.

Section 4 creates s. 282.3186, F.S., relating to ransomware incident compliance.

Section 5 amends s. 282.319, F.S., relating to the Florida Cybersecurity Advisory Council.

Section 6 creates s. 815.062, F.S., relating to offenses against governmental entities.

Section 7 creates an unnumbered section of law providing that the Legislature finds that the act fulfills an important state interest.

[46] The bill defines the term "government entity" to mean any official, officer, commission, board, authority, council, committee, or department of the executive, judicial, or legislative branch of state government; state universities; and any county or municipality, special district, water management district, and any other district in this state.

Section 8 provides an effective date of July 1, 2022.

II. FISCAL ANALYSIS & ECONOMIC IMPACT STATEMENT

A. FISCAL IMPACT ON STATE GOVERNMENT:

1. Revenues:

   The bill establishes a punitive fine for a person convicted of a ransomware offense against a government entity. Moneys recovered pursuant to the punitive fine are to be deposited into the General Revenue Fund. Accordingly, the bill may have an indeterminate positive fiscal impact on the state.

2. Expenditures:

   The bill places additional requirements on state agencies including submitting after action-reports and providing cybersecurity training on an annual basis. In addition, the bill expands the functions of the CAC to include advising counties and municipalities on cybersecurity, and prohibits state agencies from paying or otherwise complying with a ransomware incident ransom. *See* Fiscal Comments.

B. FISCAL IMPACT ON LOCAL GOVERNMENTS:

1. Revenues:

   None.

2. Expenditures:

   The bill places a number of requirements on local governments regarding cybersecurity, including completing cybersecurity trainings, adopting cybersecurity standards, reporting ransomware and certain cybersecurity incidents, and submitting after-action reports. In addition, the bill prohibits certain local governments from paying or otherwise complying with a ransomware incident ransom. *See* Fiscal Comments.

C. DIRECT ECONOMIC IMPACT ON PRIVATE SECTOR:

None.

D. FISCAL COMMENTS:

The proposed House of Representatives FY 2022-2023 General Appropriations Act (GAA) is anticipated to:

- Fund $30 million in nonrecurring General Revenue for DMS to administer a grants program that provides cybersecurity technical assistance to counties and municipalities,
- Fund $5,428,240 in federal trust fund budget authority for DMS to distribute cybersecurity assistance grants from the federal Infrastructure Investment and Jobs Act based on guidance provided by the Cybersecurity and Infrastructure Security Agency and the Federal Emergency Management Agency [47],
- Transfer $7 million in nonrecurring General Revenue to the Florida Center for Cybersecurity at the University of South Florida, in consultation with the Florida Cybersecurity Advisory Council, to conduct a comprehensive assessment of the state's critical infrastructure and provide recommendations for improvement of the state's preparedness and resilience to significant cybersecurity incidents, and
- Transfer $30 million in nonrecurring General Revenue to the Florida Center for Cybersecurity at the University of South Florida, in consultation with DMS and the Florida Cybersecurity Advisory

[47] Infrastructure Investment and Jobs Act, Pub. L. No. 117-58, H.R. 3684, 117th Cong. (11/15/2021). This funding is contingent on federal grants being awarded.

Council, to provide cybersecurity training to state and local government executive, managerial, technical, and general staff.

III. COMMENTS

A. CONSTITUTIONAL ISSUES:

1. Applicability of Municipality/County Mandates Provision:

The county/municipality mandates provision of Art. VII, s. 18 of the Florida Constitution may apply because the bill places cybersecurity related requirements on local governments, including completing cybersecurity trainings, adopting cybersecurity standards, reporting ransomware and certain cybersecurity incidents, and submitting after-action reports; however, an exemption may apply if the costs related to those cybersecurity requirements are insignificant. An exception may apply because similarly situated entities are required to comply with the same cybersecurity requirements and the bill provides an important state interest determination. An exception may also apply because the General Appropriations Act provides estimated funds to cover the mandate.

2. Other:

None.

B. RULE-MAKING AUTHORITY:

The bill grants rulemaking authority to FLDS to establish guidelines and processes for local governments to use when submitting after-action reports.

C. DRAFTING ISSUES OR OTHER COMMENTS:

None.

IV. AMENDMENTS/COMMITTEE SUBSTITUTE CHANGES

On February 23, 2022, the State Affairs Committee adopted a proposed committee substitute (PCS) and reported the bill favorably as a committee substitute. The PCS differed from the bill in that it:

- Defined the level of severity of a cybersecurity incident in accordance with the U.S. Department of Homeland Security's National Cyber Incident Response Plan;
- Required the advanced cybersecurity training offered to specified state agency and local government employees to include training on the cybersecurity incident severity levels;
- Differentiated reporting requirements based on the level of severity of a cybersecurity incident;
- Required the Legislature to only be notified of high severity level cybersecurity incidents; and
- Required the CSOC to provide the Legislature and CAC with a consolidated incident report on a quarterly basis.

This analysis is drafted to the committee substitute adopted by the State Affairs Committee.