HOUSE OF REPRESENTATIVES STAFF ANALYSIS

BILL #: CS/CS/HB 1555 Cybersecurity
SPONSOR(S): State Administration & Technology Appropriations Subcommittee, Energy, Communications & Cybersecurity Subcommittee, Giallombardo
TIED BILLS: **IDEN./SIM. BILLS:** SB 1662

REFERENCE	ACTION	ANALYST	STAFF DIRECTOR or BUDGET/POLICY CHIEF
1) Energy, Communications & Cybersecurity Subcommittee	15 Y, 0 N, As CS	Bauldree	Keating
2) State Administration & Technology Appropriations Subcommittee	13 Y, 0 N, As CS	Mullins	Topp
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 state agencies to report all ransomware incidents, regardless of severity level, to the FLDS Cybersecurity Operations Center (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; and
- Revises the mission, goals, and responsibilities of the Florida Center for Cybersecurity.

The bill has an indeterminate fiscal impact on state expenditures. *See* Fiscal Comments.

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.

Florida Center for Cybersecurity

The Florida Center for Cybersecurity (Cyber Florida) is housed within the University of South Florida (USF) and was first established in 2014.[45] The goals of Cyber Florida are to:[46]

- Position Florida as the national leader in cybersecurity and its related workforce through education, research, and community engagement.
- Assist in the creation of jobs in the state's cybersecurity industry and enhance the existing cybersecurity workforce.
- Act as a cooperative facilitator for state business and higher education communities to share cybersecurity knowledge, resources, and training.
- Seek out partnerships with major military installations to assist, when possible, in homeland cybersecurity defense initiatives.

[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.
[45] Ch. 2014-56, L.O.F.
[46] S. 1004.444, F.S.

- Attract cybersecurity companies to the state with an emphasis on defense, finance, health care, transportation, and utility sectors.

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.
- “Criminal Justice Agency” has the same meaning as defined in 943.045 (11).

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.

DMS and FLDS Duties

The bill revises the duties of FLDS to include:

- Leading enterprise IT and cybersecurity efforts.
- Propose and evaluate solutions pursuant to interagency agreements 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 gives FLDS the authority to obtain immediate and complete access to state agency accounts and instances that hold enterprise digital data and to direct, in consultation with the state agency that holds the particular data, measures to assess, monitor, and protect the security of such data. The department is not authorized to view, modify, transfer, or otherwise duplicate enterprise digital data except as required to respond to a cyber incident or as agreed to in writing by the state agency that holds the particular enterprise digital data. The bill exempts all criminal justice entities from this FLDS access authorization.

State Agency Incident Reporting and Responsibilities

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.

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 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 FDLE, President of the Senate, Speaker of the House of Representatives, and the CAC.

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.

Local Government Incident Reporting and Responsibilities

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.

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.

Florida Center for Cybersecurity (Cyber Florida)

The bill provides that the Florida Center for Cybersecurity may also be referred to as "Cyber Florida." The bill clarifies that Cyber Florida is under the direction of the president of USF or the president's designee. Under the bill, the USF president may assign Cyber Florida to a college of USF if the college has a strong emphasis in cybersecurity, technology, or computer sciences and engineering as determined and approved by USF's board of trustees.

The bill revises Cyber Florida's mission and goals to be:

- Position Florida as the national leader in cybersecurity and its related workforce primarily through advancing and funding education, and research and development initiatives in cybersecurity and related fields, with a secondary emphasis on, and community engagement and cybersecurity awareness;
- Assist in the creation of jobs in the state's cybersecurity industry and enhance the existing cybersecurity workforce through education, research, applied science, and engagements and partnerships with the private and military sectors;
- Act as a cooperative facilitator for state business and higher education communities to share cybersecurity knowledge, resources, and training;

- Seek out research and development agreements and other partnerships with major military installations and affiliated contractors to assist, when possible, in homeland cybersecurity defense initiatives;
- Attract cybersecurity companies and jobs to the state with an emphasis on defense, finance, health care, transportation, and utility sectors; and
- Conduct, fund, and facilitate research and applied science that leads to the creation of new technologies and software packages that have military and civilian applications and which can be transferred for military and homeland defense purposes or for sale or use in the private sector.

The bill provides that if Cyber Florida receives a request for assistance from DMS, FLDS, or another state agency, Cyber Florida is authorized, but may not be compelled by the agency, to conduct, consult on, or otherwise assist any state-funded initiatives related to:

- Cybersecurity training, professional development, and education for state and local government employees, including school districts and the judicial branch.
- Increasing the cybersecurity effectiveness of the state's and local governments' technology platforms and infrastructure, including school districts and the judicial branch.

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. 282.318, F.S., relating to cybersecurity.

Section 5: Amends s. 282.3185, F.S., relating to local government cybersecurity.

Section 6: Amends s. 1004.444, F.S., relating to Florida Center for Cybersecurity.

Section 7: Provides an effective date.

II. FISCAL ANALYSIS & ECONOMIC IMPACT STATEMENT

A. FISCAL IMPACT ON STATE GOVERNMENT:

1. Revenues:

   None.

2. Expenditures:

   See Fiscal Comments.

B. FISCAL IMPACT ON LOCAL GOVERNMENTS:

1. Revenues:

   None.

2. Expenditures:

   None.

C. DIRECT ECONOMIC IMPACT ON PRIVATE SECTOR:

None.

D. FISCAL COMMENTS:

The bill has an indeterminate but likely significant fiscal impact. DMS may have costs related to systems integration and process automation services necessary to receive all agency cybersecurity incidents and to obtain the immediate CSOC cybersecurity incident notifications proposed in the bill.

According to DMS, the Chief Technology Officer established in the bill can be created utilizing an existing position and within current resources.[47]

According to FDLE, state agencies may incur additional workload of reporting all cybersecurity incidents as proposed in the bill. [48]

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:

[47] Email from Jake Holmgreen, Deputy Legislative Affairs Director, Department of Management Services, FW: Chief Technology Officer Position in HB 1555 (Feb. 13, 2024).

[48] Florida Department of Law Enforcement, Agency Analysis of 2024 House Bill 1555, p. 5 (Jan. 30, 2024).

The bill does not require or authorize rulemaking.

C. DRAFTING ISSUES OR OTHER COMMENTS:

1. Lines 100 to 102 provide a definition for "as a service". This definition was only used for the original bill language that was removed in an amendment adopted by the Energy, Communications & Cybersecurity Subcommittee on January 25, 2024. The definition no longer applies to the current committee substitute.
2. Lines 103 to 104 provide a definition for "cloud provider". The bill does not use this term, nor is the term included in current statute.

IV. AMENDMENTS/COMMITTEE SUBSTITUTE CHANGES

On January 25, 2024, the Energy, Communications & Cybersecurity Subcommittee adopted three amendments and reported the bill favorably as a committee substitute. The amendments:

- Remove provisions of the bill that designate certain information security personnel positions as select exempt positions.
- Remove provisions of the bill that require each state agency head to designate a CISO and that specify how an agency's information security manager must interact with the agency CISO.
- Update the mission, goals, and responsibilities of the Florida Center for Cybersecurity ("Cyber Florida") housed within USF and authorize the USF president to assign the Center to an appropriate college within the university, with approval of the board of trustees.

On February 13, 2024, the State Administration and Technology Appropriations Subcommittee adopted an amendment and reported the bill favorably as a committee substitute. The amendment:

- Adds a definition for "criminal justice agency" and revises the definition of "enterprise digital data".
- Revises the duties of the FLDS.
- Removes provisions of the bill that changes FLDS' project oversight responsibilities.
- Removes provisions of the bill that repeals the responsibility for FLDS to conduct an annual market analysis.
- Removes provisions of the bill that repeals the requirement for the FLDS to execute a data sharing agreement with an agency in order to disclose or retrieve that agency's data.
- Clarifies the provisions of the bill that changes the CSOC incident notification process.
- Removes provisions of the bill that clarifies how and when the President of the Senate and the Speaker of the House of Representatives would be notified of cybersecurity incidents and ransomware.
- Removes provisions of the bill that specifies how the Legislature would be briefed on cybersecurity and who in the Legislature is authorized to receive these briefings.

This analysis is drafted to the committee substitute as passed by the State Administration and Technology Appropriations Subcommittee.