HOUSE OF REPRESENTATIVES STAFF FINAL BILL ANALYSIS

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

FINAL HOUSE FLOOR ACTION: 112 **Y's** 0 **N's** **GOVERNOR'S ACTION:** Approved

SUMMARY ANALYSIS

CS/CS/CS/HB 1555 passed the House on March 4, 2024. The bill was amended in the Senate on March 5, 2024, and returned to the House. The House concurred in the Senate amendment and subsequently passed the bill as amended on March 7, 2024.

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 Florida Center for Cybersecurity is housed within the University of South Florida (USF) and was first established in 2014. The mission of the Center includes positioning Florida and its related workforce as the national leader in cybersecurity through education, research, and community engagement.

The bill provides that the Florida Center for Cybersecurity at USF may be referred to as "Cyber Florida" and revises its mission and goals. The bill adds the following new mission: 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.

Additionally, 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 does not appear to have a fiscal impact on state or local government revenues or expenditures.

The bill was approved by the Governor on April 15, 2024, ch. 2024-99, L.O.F., and will become effective on July 1, 2024.

I. SUBSTANTIVE INFORMATION

A. EFFECT OF 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 DMS and was established in 2020 to replace the Division of State Technology.[11] FLDS works under

---

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

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]

Florida Center for Cybersecurity

The Florida Center for Cybersecurity is housed within the University of South Florida (USF) and was first established in 2014.[18] The goals of the Center are to:[19]

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

Effect of the Bill

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.

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

[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. 2014-56, L.O.F.
[19] S. 1004.444, F.S.

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.

II. FISCAL ANALYSIS & ECONOMIC IMPACT STATEMENT

FISCAL IMPACT ON STATE GOVERNMENT:

1. Revenues:

   None.

2. Expenditures:

   None.

A. FISCAL IMPACT ON LOCAL GOVERNMENTS:

1. Revenues:

   None.

2. Expenditures:

   None.

B. DIRECT ECONOMIC IMPACT ON PRIVATE SECTOR:

None.

C. FISCAL COMMENTS:

None.