HOUSE OF REPRESENTATIVES STAFF FINAL BILL ANALYSIS

BILL #: CS/CS/HB 1297 Cybersecurity
SPONSOR(S): State Affairs Committee; Government Operations Subcommittee; Giallombardo, Byrd and others
TIED BILLS: **IDEN./SIM. BILLS:** CS/CS/SB 1900

FINAL HOUSE FLOOR ACTION: 118 **Y's** 0 **N's** **GOVERNOR'S ACTION:** Approved

SUMMARY ANALYSIS

CS/CS/HB 1297 passed the House on April 15, 2021, and subsequently passed the Senate on April 27, 2021.

The Information Technology (IT) Security Act requires the Department of Management Services (DMS) and the heads of state agencies to meet certain requirements to enhance the IT security of state agencies. It provides that DMS is responsible for establishing standards and processes consistent with generally accepted best practices for IT security and adopting rules that safeguard an agency's data, information, and IT resources to ensure availability, confidentiality, and integrity and to mitigate risks.

The bill specifies that DMS, acting through the Florida Digital Service (FDS), is the lead entity responsible for assessing state agency cybersecurity risks and determining appropriate security measures. The bill creates new, and amends current, cybersecurity duties and responsibilities of DMS. The new responsibilities include:

- Developing and publishing guidelines and processes for state agencies to use when procuring IT commodities and services to ensure the commodity or service meets the National Institute for Standards and Technology cybersecurity framework.
- Providing cybersecurity training to all state agency technology professionals.
- Operating and maintaining a Cybersecurity Operations Center to serve as a clearinghouse for threat information and to coordinate with the Florida Department of Law Enforcement (FDLE) to support state agency response to cybersecurity incidents.

The bill directs each agency inspector general to include a specific cybersecurity audit plan when developing its long-term and annual audit plans.

Further, the bill creates the Florida Cybersecurity Advisory Council within DMS. The purpose of the council is to assist state agencies in protecting IT resources from cyber-attacks. The council is required to meet 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 the FDS in developing cybersecurity best practice recommendations, and examine inconsistencies between state and federal law regarding cybersecurity. The bill specifies the membership of the council and requires the council to submit annually any cybersecurity legislative recommendations it considers necessary to address cybersecurity to the President of the Senate and the Speaker of the House of Representatives beginning June 30, 2022.

SB 2500, the General Appropriations Act for fiscal year 2021-2022, provides 15 full time equivalent cybersecurity positions and $30 million from the General Revenue Fund to implement the provisions of the bill and the recommendations of the final report of the Florida Cybersecurity Task Force. The appropriation is contingent upon HB 1297 or similar legislation becoming a law.

The bill was approved by the Governor on June 29, 2021, ch. 2021-234, L.O.F., and will become effective on July 1, 2021.

I. SUBSTANTIVE INFORMATION

A. EFFECT OF CHANGES:

Background

Cybersecurity Attacks

Over the last decade, cybersecurity has rapidly become a growing concern. According to a report from Cybersecurity Ventures, a leading researcher in the cybersecurity industry, cybercrime is expected to inflict $6 trillion worth of damage globally in 2021.[1] The United States is often a target of cyber-attacks and has received more significant cyber-attacks[2] over the last 14 years than any other country. Below are examples of recent cybersecurity incidents that involved the U.S.:

- January 2021: Hackers linked to Hezbollah breached telecom companies, internet service providers, and hosting providers in the U.S. and other countries.
- December 2020: The Cybersecurity and Infrastructure Security Agency and the Federal Bureau of Investigations announced that U.S. think tanks focusing on national security and international affairs were being targeted by state-sponsored hacking groups.
- October 2020: Iranian hackers targeted state election websites in order to download voter registration information and conduct voter intimidation campaigns.
- October 2020: A Russian hacking group breached the U.S. state and local government networks, as well as aviation networks, and exfiltrated data.
- October 2020: The National Security Agency announced that Chinese government hackers were targeting the U.S. defense industrial base as part of a wide-ranging espionage campaign.
- September 2020: The Cybersecurity and Infrastructure Security Agency revealed that hackers associated with the Chinese Ministry of State Security had been scanning U.S. government and private networks for over a year in search of networking devices that could be compromised.
- August 2020: An Iranian hacking group was found to be targeting major U.S. companies and government agencies by exploiting recently disclosed vulnerabilities in high-end network equipment to create backdoors for other groups to use.
- July 2020: Canada, the United Kingdom, and the U.S. announced that hackers associated with Russian intelligence had attempted to steal information related to Covid-19 vaccine development.[3]

In an effort to protect against cyber-attacks, organizations typically employ a CIA triad strategy, which stands for confidentiality, integrity, and availability. The CIA triad is so essential to cybersecurity that anytime there is a breach, it is likely because one or more of these principles have been violated. Security professionals evaluate threats and vulnerabilities based on the potential impact they have on the confidentiality, integrity, and availability of an organization's assets. The individual components of the CIA triad are explained below:

- Confidentiality refers to an organization's efforts to keep their data private or secret. Typically, this involves ensuring that only those who are authorized have access to specific assets and that those who are unauthorized are actively prevented from obtaining access.
- Integrity is about ensuring that data has not been tampered with and, therefore, can be trusted; it ensures that the data is correct, authentic, and reliable.
- Availability means that networks, systems, and applications are up and running; it ensures that authorized users have timely, reliable access to resources when they are needed.[4]

---

[1] Cybercrime Magazine, *Cybercrime to Cost the World $10.5 Trillion Annually by 2025*, https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/ (last visited March 1, 2021).

[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.

[3] Center for Strategic & International Studies, *Significant Cyber Incidents*, https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents (last visited March 1, 2021).

[4] F5 Labs Application Threat Intelligence, *What is the CIA Triad?*, https://www.f5.com/labs/articles/education/what-is-the-cia-triad (last visited March 1, 2021).

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 U.S. 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]

Information Technology Management

The Department of Management Services (DMS)[7] oversees information technology (IT)[8] governance and security for the executive branch of state government. The Florida Digital Service (FDS), within DMS, established in 2020 to replace the Division of State Technology,[9] implements DMS' duties and policies in this area.[10]

The head of FDS is appointed by the Secretary of Management Services[11] and serves as the state chief information officer (CIO).[12] The CIO must have at least five years of experience in the development of IT system strategic planning and development of IT policy and, preferably, have leadership-level experience in the design, development, and deployment of interoperable software and data solutions.[13] FDS proposes 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.[14]

DMS, through FDS, 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.
- 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.

Information Technology Security Act

---

[5] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (last visited March 1, 2021).
[6] *Id*.
[7] *See* s. 20.22, F.S.
[8] 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(19), F.S.
[9] Ch. 2020-161, L.O.F.
[10] *See* s. 20.22(2)(b), F.S.
[11] 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.
[12] Section 282.0051(2)(a), F.S.
[13] *Id*.
[14] Section 282.0051(1), F.S.

The IT Security Act[15] requires DMS and the heads of state agencies[16] to meet certain requirements to enhance the IT security of state agencies. Specifically, the IT Security Act provides that DMS is responsible for establishing standards and processes consistent with generally accepted best practices for IT security,[17] including cybersecurity, and adopting rules that safeguard an agency's data, information, and IT resources to ensure availability, confidentiality, and integrity and to mitigate risks.[18] In addition, DMS must:

- Designate a state chief information security officer (CISO) to oversee state IT security.
- Develop, and annually update, a statewide IT security strategic plan.
- Develop and publish an IT security framework for use by state agencies.
- Collaborate with the Cybercrime Office within the Florida Department of Law Enforcement (FDLE) in providing training for state agency information security managers and computer security incident response team members.
- Annually review the strategic and operational IT security plans of executive branch agencies.[19]

The IT Security Act requires the head of each state agency to designate an information security manager to administer the IT security program of the state agency.[20] In addition, the head of each state agency must:

- Establish an agency computer incident response team in consultation with the Cybercrime Office within FDLE.
- Annually submit to DMS the state agency's strategic and operational IT security 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 IT security incidents and breaches to the Cybercrime Office within FDLE and FDS.
- Ensure that periodic internal audits and evaluations of the agency's IT security program for the data, information, and IT resources of the agency are conducted.
- Ensure that the IT security and cybersecurity requirements in both written specifications for the solicitation and service-level agreement of IT and IT resources and services meet or exceed applicable state and federal laws, regulations, and standards for IT security and cybersecurity.
- Provide IT security and cybersecurity awareness training to all state agency employees within 30 days of commencing employment.
- Develop a process that is consistent with the rules and guidelines established by DMS for detecting, reporting, and responding to threats, breaches, or IT security incidents.[21]

Advisory Council

Under Florida law, an "advisory council" means an advisory body created by specific statutory enactment and appointed to function on a continuing basis.[22] Generally, an advisory council is enacted to study the problems arising in a specified functional or program area of state government and to provide recommendations and policy alternatives.[23]

---

[15] Section 282.318, F.S.

[16] The term "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 or state universities. Section 282.0041(33), F.S. For purposes of the IT Security Act, the term 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.

[17] The term "information technology security" means the protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of data, information, and information technology resources. Section 282.0041(22), F.S.

[18] Section 292.318(3), F.S.

[19] *Id*.

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

[21] Section 282.318(4), F.S.

[22] Section 20.03(7), F.S.

[23] *Id*.

Florida law provides the following requirements for statutorily enacted advisory councils:

- A council may only be created when it is found to be necessary and beneficial to the furtherance of a public purpose.
- An advisory council may not be created or reestablished unless it meets a statutorily defined purpose and its powers conform to the definition of "advisory council" under law.
- An advisory council must be terminated by the Legislature when it is no longer necessary and beneficial to the furtherance of a public purpose. The executive agency to which the advisory council is made an adjunct must advise the Legislature at the time the committee ceases to be essential to the furtherance of a public purpose.
- The Legislature and the public must be kept informed of the numbers, purposes, memberships, activities, and expenses of the committee.[24]

A private citizen member of an advisory council that is adjunct to an executive agency must be appointed by the Governor, the head of the department, the executive director of the department, or a Cabinet officer.[25]

Advisory council members are subject to the Code of Ethics for Public Officers and Employees (Code) set forth in part III, ch. 112, F.S. The Code is intended to ensure that public officers[26] conduct themselves independently and impartially, not using their office for private gain other than compensation provided by law.[27] As such, the Code prohibits certain actions or conduct of council members, including prohibitions on the solicitation or acceptance of gifts, unauthorized compensation, misuse of their public position, and disclosure or use of information gained as a result of their membership.[28]

Effect of the Bill

The bill defines "cybersecurity" to mean 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.

The bill specifies that DMS, acting through the Florida Digital Service (FDS), is the lead entity responsible for assessing state agency cybersecurity risks and determining appropriate security measures. The bill creates new, and amends current, cybersecurity duties and responsibilities assigned to DMS. Specifically, DMS, acting through FDS, must:

- Establish standards and processes consistent with generally accepted best practices for IT security, including the NIST cybersecurity framework.
- Adopt rules to mitigate risk, support a security governance framework, and safeguard state agency digital assets, data, information, and IT resources to ensure availability, confidentiality, and integrity.
- Designate a chief information security officer (CISO) responsible for the development, operation, and oversight of cybersecurity. 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 state chief information officer (CIO) and the Governor.
- Develop and annually update a statewide cybersecurity plan that includes the identification and mitigation of risk, proactive protections against threats, tactical risk detection, threat reporting, and response and recovery protocols for cyber incidents.

[24] Section 20.052(1)-(4), F.S.
[25] Section 20.052(5)(a), F.S.
[26] The term "public officer" includes any person elected or appointed to hold office in any agency, including any person serving on an advisory body. Section 112.313(1), F.S.
[27] Section 112.311(1), F.S.
[28] Section 112.313, F.S.

- Develop and publish a cybersecurity governance framework that must include guidelines and processes for state agencies to use when procuring IT commodities and services to ensure the commodity or service meets the NIST cybersecurity framework.
- 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.
- 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.

The bill directs each agency inspector general to include a specific cybersecurity audit plan when developing its long-term and annual audit plans. In addition, the bill provides that if a private sector vendor is used to complete an agency's comprehensive risk assessment, the vendor must attest to the validity of the risk assessment findings.

The bill authorizes a state agency's employee cybersecurity awareness training to be provided in collaboration with a private sector entity or an institution of the state university system.

The bill creates the Florida Cybersecurity Advisory Council within DMS. The purpose of the council is to assist state agencies in protecting IT resources from cyber threats and incidents. The council will assist FDS in implementing best cybersecurity practices, taking into consideration the final recommendations of the Florida Cybersecurity Task Force. The council must meet 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 the FDS in developing cybersecurity best practice recommendations including continuous risk monitoring, password management, and protecting data in legacy and new systems.
- Examine inconsistencies between state and federal law regarding cybersecurity.

The council must also 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.

The bill requires council members to maintain the confidential or exempt status of information received in the performance of their official duties and responsibilities. It prohibits current or former members from disclosing or using information not available to the public and gained by reason of their official position for their personal gain or benefit or the personal gain or benefit of another. Council members must sign an agreement acknowledging these provisions.

The council will be comprised of the following members:

- The Lieutenant Governor or his or her designee.
- The state CIO.
- The state CISO.
- The director of the Division of Emergency Management.
- A representative of the Computer Crime Center of FDLE, appointed by the executive director of FDLE.
- A representative of the Florida Fusion Center of FDLE, appointed by the executive director of FDLE.
- The Chief Inspector General.

- A representative from the Public Service Commission.
- Up to two representatives from institutions of higher education located in the state, appointed by the Governor.
- Three representatives from critical infrastructure sectors, one of which 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.
- 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.

The bill provides for four-year staggered terms and provides that the members serve without compensation, but are entitled to reimbursement for per diem and travel expenses.

The bill requires the DMS Secretary or his or her designee to serve as an ex officio, nonvoting executive director of the council.

Beginning June 30, 2022, and each June 30 thereafter, the council must submit to the Legislature any cybersecurity legislative recommendations considered necessary by the council to address cybersecurity.

II. FISCAL ANALYSIS & ECONOMIC IMPACT STATEMENT

A. FISCAL IMPACT ON STATE GOVERNMENT:

1. Revenues:

   None.

2. Expenditures:

   The bill will have a significant fiscal impact on state government due to the operation and maintenance of the Cybersecurity Operations Center, increased frequency of comprehensive risk assessments by state agencies, and expenses associated with FDS and the Florida Cybersecurity Advisory Council.

   SB 2500, which is the Fiscal Year 2021-22 General Appropriations Act (GAA), requires FDS, from funding provided to the Office of the Chief Information Officer, to incorporate the recommendations of the Florida Cybersecurity Task Force Final Report into an implementation plan developed as part of the statewide IT security strategic plan pursuant to s. 282.318(3)(b), F.S. To implement the recommendations of the Florida Cybersecurity Task Force Final Report, SB 2500 also provides to FDS:
   - 15 full time equivalent cybersecurity positions; and
   - $30 million from the General Revenue Fund, which includes:
     - $3,200,000 for Cybersecurity Assessments and an Asset Inventory;
     - $2,244,576 for Endpoint Protection Software and Services;
     - $1,000,000 for Agency Inspectors General Auditing Resources;
     - $2,400,000 for .gov Domain Protection Software;
     - $400,000 for Governance Repository Software;
     - $2,400,000 for Identity Management Software;
     - $2,400,000 for Industrial Control System/Critical Infrastructure Hardening;
     - $1,600,000 for Cybersecurity Intelligence Software and Services;
     - $3,200,000 for the Cybersecurity Operations Center;
     - $320,000 for Centralized Service Delivery Tracking Software;
     - $4,291,920 for Security Information and Event Management Software and Services;

- $698,579 for Cybersecurity Training;
- $4,020,400 for Vulnerability Management; and
- $1,824,525 for Information Technology Audit Findings.

The FY 2021-22 GAA provides that the $30 million appropriation is contingent upon HB 1297 or similar legislation becoming a law.

B. FISCAL IMPACT ON LOCAL GOVERNMENTS:

1. Revenues:

None.

2. Expenditures:

None.

C. DIRECT ECONOMIC IMPACT ON PRIVATE SECTOR:

None.

D. FISCAL COMMENTS:

None.