The Florida Senate

BILL ANALYSIS AND FISCAL IMPACT STATEMENT

(This document is based on the provisions contained in the legislation as of the latest date listed below.)

Prepared By: The Professional Staff of the Committee on Governmental Oversight and Accountability

BILL:	CS/SB 1900
INTRODUCER:	Governmental Oversight and Accountability Committee and Senator Boyd
SUBJECT:	Cybersecurity
DATE:	March 31, 2021 REVISED:

	ANALYST	STAFF DIRECTOR	REFERENCE	ACTION
1.	Candelaria	McVaney	GO	**Fav/CS**
2.			AEG	
3.			AP	

Please see Section IX. for Additional Information:

COMMITTEE SUBSTITUTE - Substantial Changes

I. Summary:

CS/SB 1900 expands the duties and responsibilities of the Florida Digital Service (FDS) relating to the state's cybersecurity governance framework.

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 requires that a cybersecurity audit plan be included in the long-term and annual audit plan that agency inspectors general are required to complete.

The bill designates the FDS as the lead entity responsible for assessing state agency cybersecurity risks and determining appropriate security measures to combat such risks. The bill creates, and amends current, cybersecurity related duties and responsibilities of the Department of Management Services (DMS). The bill also expands the responsibilities of each state agency head in relation to cybersecurity.

The bill creates the Florida Cybersecurity Advisory Council (Council) within the DMS. The purpose of the Council is to assist the state in protecting the state's information technology resources from cyber threats and incidents, and to assist the FDS in implementing best cybersecurity practices. The bill outlines membership requirements of the Council, term requirements of each member, and duties and responsibilities of the Council as a whole.

Beginning June 30, 2022, and annually thereafter, the Council is required to submit a report to the Governor, the President of the Senate, and the Speaker of the House of Representatives outlining any recommendations considered necessary by the Council to address cybersecurity.

The bill makes conforming changes across several provisions by replacing all versions of the term "information technology security" with the term "cybersecurity."

The bill takes effect July 1, 2021.

II. Present Situation:

Agency Inspectors General

An office of the inspector general (Office) is established in each state agency to provide a central point for coordination of, and responsibility for, activities that promote accountability, integrity, and efficiency in government.[1] The Office within each agency is responsible for advising in the development of performance measures, standards, and procedures for the evaluation of state agency programs. The Office is also required to assess the reliability and validity of information provided by the state agency on performance measures and standards and must make recommendations for improvement when necessary.

In carrying out the auditing duties and responsibilities, each inspector general should review and evaluate internal controls necessary to ensure the fiscal accountability of the state agency. The inspector general will conduct financial, compliance, electronic data processing, and performance audits of the agency and prepare audit reports of the findings. At the conclusion of an audit, the inspector general will submit preliminary findings and recommendations to the person responsible for supervision of the program function or operational unit who can respond to any adverse findings within 20 working days after receipt of the preliminary findings. The inspector general will submit the final report to the agency head, the Auditor General and, for state agencies under the Governor, the Chief Inspector General. The inspector general shall develop long-term and annual audit plans based on the findings of the risk assessment. The plan, where appropriate, should include post-audit samplings of payments and accounts. The plan should show the individual audits to be conducted during each year and related resources to be devoted to the respective audits. A copy of the approved plan shall be submitted to the Auditor General.[2]

National Institute for Standards and Technology Cybersecurity Framework

The National Institute for Standards and Technology Cybersecurity (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

[1] Section 20.055(2), F.S.
[2] *Id.*

organizations in any sector of the economy or society.[3] 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. Overall, the framework provides an outline of best practices that helps organizations decide where to focus resources for cybersecurity protection.[4]

The Information Technology Act

The Information Technology Act (Act) establishes that the Department of Management Services (DMS) is responsible for establishing standards and processes consistent with generally accepted best practices for information technology (IT) security, including cybersecurity, and adopting rules that safeguard an agency's data, information, and IT resources to mitigate risks.[5] The DMS is required to designate an employee of the Florida Digital Service (FDS) as the state chief information security officer, who must have experience and expertise in security and risk management for communications and IT resources.

The DMS is required, by February 1 of each year, to develop a statewide IT security strategic plan that includes security goals and objectives for the strategic issues of IT security policy, risk management, training, and disaster recovery planning. Further, the DMS is required to develop and publish for use by state agencies an information technology security framework that includes specific guidelines and processes.[6]

The DMS, in collaboration with the Cybercrime Office of the Department of Law Enforcement, provides training for state agency information security managers and computer security incident response team members that contains training on IT security.[7] The DMS is required to develop and publish for use by state agencies an IT security framework. The Act requires each state agency to designate an information security manager to administer the IT security program of the state agency. This designation must be provided annually in writing to the DMS.[8]

Florida Digital Service

The FDS has been created within the DMS to propose innovative solutions that securely modernize state government, including technology and information services, to achieve value through digital transformation, and to fully support cloud-first policy[9]. The FDS partners with all state agencies to deliver better government services through design and technology. The FDS is responsible for developing an enterprise architecture, project management and oversight standards, and technology policy for the management of the state's IT[10] resources.

---

[3] 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 30, 2021).
[4] *Id.*
[5] Section 282.318, F.S.
[6] Section 282.318(3)(b), F.S.
[7] Section 282.318(3)(e), F.S.
[8] *Id.*
[9] Section 282.0051(1), F.S.
[10] Section 282.0041(1), F.S., defines "information technology" to mean equipment, hardware, software, firmware, programs, systems, networks, infrastructure, media, and related material used to automatically, electronically, and wirelessly collect,

The Secretary of the DMS is required to designate a state chief information officer, who will administer the FDS. The state chief information officer must have at least five years of experience in the development of IT strategic planning and development or IT policy, and preferably have leadership-level experience in the design, development, and deployment of interoperable software and data solutions. The state chief information officer, on consultation with the Secretary of the DMS, is required to designate a state chief data officer. The chief data officer must be a proven and effective administrator who must have significant and substantive experience in data management, data governance, interoperability, and security.

Florida Center for Cybersecurity

Section 1004.444, F.S., creates the Florida Center for Cybersecurity (Cyber Florida).[11] Cyber Florida was created to help the state become a national leader in cybersecurity education, academics, practical research, and community outreach. Established under the auspices of the University of South Florida, Cyber Florida works with all 12 State University System institutions to:

- 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; and
- Attract cybersecurity companies to the state with an emphasis on defense, finance, health care, transportation, and utility sectors.[12]

State Data Center

The State Data Center (Data Center) within the DMS provides data center services that comply with applicable state and federal laws, regulations, and policies, including all applicable security, privacy, and auditing requirements.[13] The Data Center offers, develops, and supports the services and applications defined in service-level agreements executed with its customer entities. The Data Center enters into service-level agreements with each customer entity to provide the required type and level of service or services.

Cybercrime Office

The cybercrime office is created within the Department of Law Enforcement (FDLE). The cybercrime office may investigate violations of state law pertaining to the sexual exploitation of children which are facilitated or connected to the use of any device capable of storing electronic data. The cybercrime office monitors state IT resources and provides analysis on IT security incidents, threats, and breaches as defined in s. 282.0041, F.S. Further, the cybercrime office

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.

[11] Section 1004.444, F.S.

[12] *Id.*

[13] Section 282.201, F.S.

provides security awareness training and information to state agency employees concerning cybersecurity, online sexual exploitation of children, and the responsibility of employees to comply with policies, standards, guidelines, and operating procedures adopted by the FDLE. The cybercrime office consults with the FDS in the adoption of rules relating to the information technology security provisions in s. 282.318, F.S.[14]

Advisory Council Requirements under Section 20.03, Florida Statutes

Section 20.03(7), F.S., defines a "council" or "advisory council" to mean a body created by specific statutory enactment and appointed to function on a continuing basis for the study of problems arising in a specified functional or program area of state government and to provide recommendations and policy alternatives.[15]

III. Effect of Proposed Changes:

Section 1 amends s. 20.055, F.S., to require that a specific cybersecurity audit plan be included in the long-term and annual audit plan that agency inspector generals are required to complete.

Section 2 amends s. 282.0041, F.S., to substitute the term "cybersecurity" for "information technology security" and to define the term "cybersecurity" as:

> 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.

This section repeals the definition of the term "information technology security," which is made obsolete by this bill.

Sections 3, 4, and 5 amend ss. 282.0051, 282.201, and 282.206, F.S., respectively, relating to the powers and duties of DMS, the state data center, and "cloud-first" policy, to conform to the changes of the bill by replacing all versions of the term "information technology security" with the term "cybersecurity."

Section 6 amends s. 282.318, F.S., to rename the "Information Technology Security Act" as the "State Cybersecurity Act."

This section designates the DMS, acting through the FDS, as the lead entity responsible for assessing state agency cybersecurity risks and determining appropriate security measures. Thus, the DMS, acting through the FDS, must:

- Establish standards and processes that must be consistent with generally accepted technology best practices, including the National Institute for Standards and Technology (NIST) Cybersecurity Framework, for cybersecurity;
- Adopt rules that mitigate risk, safeguard the state's digital assets and agency data to ensure availability, confidentiality, and integrity and support a centralized security governance;

[14] Section 943.0415, F.S.
[15] Section 20.03(7), F.S.

- Designate an employee of the FDS as the state chief information security officer. The state chief information security officer is responsible for the development, operation, and oversight of cybersecurity for state technology systems. The state chief information security officer must be notified of all confirmed or suspected incidents or threats of state agency IT resources and must report such incidents the state chief information officer;
- Develop, and update annually by February 1, a statewide cybersecurity strategic plan that includes security goals and objectives for cybersecurity, including the identification and mitigation of risk, proactive protections against threats, tactical risk detection, threat reporting, and response and recovery protocols for a cyber incident;
- Develop and publish for use by state agencies a cybersecurity governance that includes guidelines;
- Establish procedures for procuring IT commodities and services that require the commodity or service to meet the NIST Framework;
- Provide training to all state agency technology professionals which develops, assesses, and documents competencies by role and skill level. The training may be provided in collaboration with the Cybercrime Office of the FDLE, a private sector entity, or a state university;
- Operate and maintain a Cybersecurity Operations Center led by the state chief information security officer, which must be primarily virtue and staffed with tactical detection and incident response personnel. The Cybersecurity Operations Center shall serve as a clearinghouse for threat information and will coordinate with the FDLE to support state agencies and their response to any confirmed or suspected cybersecurity incident; and
- Lead an emergency support function, ESF CYBER, under the state comprehensive emergency management plan as described in s. 252.35, F.S.

This section requires each agency head to:

- Establish an agency cybersecurity response team in consultation with the FDS and the FDLE, and must immediately report all confirmed or suspected cybersecurity incidents to the state chief information security officer, or his or her designee;
- Conduct, and update every three years, a comprehensive risk assessment which may be completed by a private sector vendor to determine security threats to the data, information, and IT resources of the agency. If a private sector vendor is used to complete this requirement, it must attest to the validity of the risk assessment findings;
- Implement managerial, operational, and risk assessment remediation plans recommended by the DMS to addresses identified risks to the agency. The FDS must track implementation by state agencies upon development of such remediation plans in coordination with agency inspectors general;
- Ensure that the cybersecurity requirements in both the written specifications for the solicitation, contracts, and service-level agreement of IT and IT resources and services meet the NIST Cybersecurity Framework; and
- Provide cybersecurity awareness training, in collaboration with the Cybercrime Office, a private sector entity, or an institution of the state university system to all state agency employees in the first 30 days after commencing employment.

This section replaces all versions of the term “information technology security” with the term “cybersecurity.”

Section 7 creates s. 282.319, F.S., establishing the Florida Cybersecurity Advisory Council (Council).

The Council must operate in a manner consistent with s. 20.052, F.S. The purpose of the Council is to assist the state in protecting the state's information technology resources from cyber threats and incidents and to assist the FDS in implementing the best cybersecurity practices, taking into consideration the final recommendations of the Florida Cybersecurity Task Force.

The Council is comprised of the following members:
- The Lieutenant Governor or his or her designee;
- The state chief information officer;
- 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 FDLE, appointed by the executive director of the DMS;
- A representative of the Florida Fusion Center of the FDLE, appointed by the executive director of the DMS;
- 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 finance, energy, health care, and transportation sector, appointed by the Governor; and
- Two representatives with expertise on emergency technology with one appointed by the President of the Senate and one appointed by the Speaker of the House of Representatives.

The members serve for a term of four years, with the initial appointments made serving for a term of two years. A vacancy must be filled for the remainder of the unexpired term in the same manner as the initial appointment, and all members of the Council are eligible for reappointment. The Secretary of Management Services, or his or her designee, must serve as the ex officio, nonvoting executive director of the Council. Members of the Council serve without compensation but are entitled to reimbursement for per diem and travel expenses as defined in s. 112.061, F.S.

The Council must meet quarterly to:
- Review existing state agency cybersecurity policies;
- Assess ongoing risks to state agency information technology;
- Recommend a method to notify state agencies of new risks;
- Recommend data breach simulation exercises;
- Examine inconsistencies between state and federal law regarding cybersecurity; and
- Assist the FDS in developing cybersecurity best practices recommendations for state agencies which include recommendations regarding:

- Continuous risk monitoring;
- Password management; and
- Protecting data in legacy and new systems.

The Council must work with the NIST and other federal agencies, private sector businesses, and private cybersecurity experts:

- For critical infrastructure not covered by federal law, to identify which local infrastructure sectors are at greatest risk of cyber attacks and need the most enhanced security measures; and
- To use federal guidance to identify categories of critical infrastructure as critical cyber infrastructure if cyber damage or access could reasonable result in catastrophic consequences.

Beginning June 30, 2022, and annually thereafter, the Council must submit a report to the Governor, the President of the Senate, and the Speaker of the House of Representatives outlining any recommendations considered necessary by the Council to address cybersecurity.

Section 8 provides the bill takes effect July 1, 2021.

IV. Constitutional Issues:

A. Municipality/County Mandates Restrictions:

The mandate restrictions do not apply because the bill does not require counties and municipalities to spend funds, reduce counties' or municipalities' ability to raise revenue, or reduce the percentage of state tax shared with counties and municipalities.

B. Public Records/Open Meetings Issues:

None.

C. Trust Funds Restrictions:

None.

D. State Tax or Fee Increases:

None.

E. Other Constitutional Issues:

None identified.

V. Fiscal Impact Statement:

A. Tax/Fee Issues:

None.

B. Private Sector Impact:

None.

C. Government Sector Impact:

The state may incur an indeterminate fiscal impact providing per diem and travel expenses for members of the newly created Florida Cybersecurity Advisory Council.

The FDS may require additional personnel, and workload, with the operation and maintenance of a Cybersecurity Operations Center, which must be staffed with tactical detection and incident response personnel.

An agency may incur additional costs if it uses a private sector vendor to complete the required risk assessment once every three years.

VI. Technical Deficiencies:

None.

VII. Related Issues:

None.

VIII. Statutes Affected:

This bill substantially amends the following sections of the Florida Statutes: 20.055, 282.0041, 282.0051, 282.201, 282.206, 282.318, and 282.319.

This bill creates the following sections of the Florida Statutes: 282.319.

IX. Additional Information:

A. Committee Substitute – Statement of Substantial Changes:
(Summarizing differences between the Committee Substitute and the prior version of the bill.)

CS by Governmental Oversight and Accountability on March 31, 2021:
The CS:

- Revises the definition for the term "Cybersecurity;"
- Removes the designation of employees under the chief information security officer as selected exempt service;
- Revises the duties of the chief information security officer from the "development, operation, and management of cybersecurity for state technology systems" to the "development, operations, and oversight of cybersecurity for state technology systems";
- Removes the authority from the Florida Digital Service to intervene in any confirmed or suspected cybersecurity incident of a state agency;

- Removes the requirement that an agency head must provide an asset management report detailing the agency's IT resources to the chief information officer and chief information security officer;
- Removes the requirement that an agency head must conduct a comprehensive risk assessment on an annual basis, and maintains the three-year requirement provided in current law;
- Requires that solicitations, contracts and service level-agreements relating to cybersecurity meet the National Institute of Standards and Technology Cybersecurity Framework;
- Revises the membership of the newly created Florida Cybersecurity Advisory Council; and
- Requires the Council to work with the National Institute of Standards and Technology, federal agencies, private sector businesses, and private cybersecurity experts to identify infrastructure vulnerable to cyber attacks.

B. Amendments:

None.