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 Appropriations

BILL:	CS/CS/CS/SB 1662
INTRODUCER:	Appropriation Committee; Appropriations Committee on Agriculture, Environment, and General Government; Governmental Oversight and Accountability Committee; and Senator Collins
SUBJECT:	Cybersecurity
DATE:	February 28, 2024
REVISED:	

	ANALYST	STAFF DIRECTOR	REFERENCE	ACTION
1.	Harmsen	McVaney	GO	**Fav/CS**
2.	Hunter	Betta	AEG	**Fav/CS**
3.	Hunter	Sadberry	AP	**Fav/CS**

Please see Section IX. for Additional Information:

COMMITTEE SUBSTITUTE - Substantial Changes

I. Summary:

CS/CS/CS/SB 1662 prohibits the award of a contract to technology services vendors that have shared information with non-United States Trade Agreements Act compliant nations without prior written consent within the past 7 years, revises the mission, goals, and responsibilities of the Florida Center for Cybersecurity and adds program oversight for the Enterprise Cybersecurity Resiliency program within the Department of Management Services.

The bill has no fiscal impact on state revenues or expenditures. See Section V., Fiscal Impact Statement.

The bill provides an effective date of July 1, 2024.

II. Present Situation:

Trade Agreements Act

Congress passed the Trade Agreements Act (TAA) of 1979 to modify provisions in the Buy American Act and to promote fair and open international trade.[1] Non-TAA compliant countries are those without trade agreements with the United States in the following categories:

- World Trade Organization Government Procurement Agreement Countries
- Free Trade Agreement Countries
- Least Developed Countries
- Caribbean Basin Countries

Non-TAA compliant countries include, but are not limited to: China, India, Indonesia, Iran, Iraq, Malaysia, North Korea, Pakistan, Russia, and Sri Lanka.[2]

Cybersecurity and Ransomware

Over the last decade, cybersecurity has rapidly become a growing concern. Cyberattacks are growing in frequency and severity. Cybercrime is expected to inflict $8 trillion worth of damage globally in 2023.[3] The United States is often a target of cyberattacks,[4] including attacks on critical infrastructure, and has been a target of more significant cyberattacks[5] over the last 14 years than any other country.[6] The Colonial Pipeline is an example of critical infrastructure that was attacked, disrupting what is arguably the nation's most important fuel conduit.[7]

Ransomware is a type of cybersecurity incident where malware[8] that is designed to encrypt files on a device and 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.

---

[1] The Department of Commerce, *The Big "A" Acquisition Conference* (May 4, 2011), The Buy American Act / Trade Agreements Act (last visited February 26, 2024).
[2] GSA Federal Schedules, *TAA Designated Countries* (Nov. 16, 2023), https://gsa.federalschedules.com/resources/taa-designated-countries/ (last visited Feb. 26, 2024).
[3] Steve Morgan, CYBERCRIME MAGAZINE, *Cybercrime to Cost the World $8 Trillion Annually in 2023* (Oct. 17, 2022), Cybercrime To Cost The World 8 Trillion Annually In 2023 (cybersecurityventures.com) (last visited Jan. 31, 2024).
[4] Chris Jaikaran, CONGRESSIONAL RESEARCH SERVICE, *Cybersecurity: Selected Cyberattacks, 2012-2022* (Aug. 9, 2023), https://crsreports.congress.gov/product/pdf/R/R46974 (last visited Jan. 25, 2024).
[5] "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. Kyle Brasseur, FRA CONFERENCES, *Study: U.S. Largest Target for Significant Cyber-Attacks* (Jul. 13, 2020), 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. 31, 2024).
[6] *Id*.
[7] 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. 31, 2024).
[8] "Malware" means hardware, firmware, or software that is intentionally included or inserted in a system for a harmful purpose. malware - Glossary | CSRC (nist.gov) (last visited Jan. 31, 2024).

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.[9] For example, Tallahassee Memorial Hospital was hit by a ransomware attack February 2023, and the hospital's systems were forced to shut down, impacting many local residents in need of medical care.[10]

Information Technology and Cybersecurity Management

The Department of Management Services (DMS) oversees information technology (IT)[11] governance and security for the executive branch in Florida.[12] The Florida Digital Service (FLDS) is housed within the DMS and was established in 2020 to replace the Division of State Technology.[13] The FLDS works under the DMS to implement policies for IT and cybersecurity for state agencies.[14]

The head of the FLDS is appointed by the Secretary of Management Services[15] and serves as the state chief information officer (CIO).[16] 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.[17] The 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.[18]

The DMS, through the FLDS, has the following powers, duties, and functions:[19]

- Develop IT policy for the management of the state's IT resources;
- Develop an enterprise architecture;
- Establish IT project management and oversight standards for state agencies;

---

[9] Cybersecurity and Infrastructure Agency, *Ransomware 101*, https://www.cisa.gov/stopransomware/ransomware-101 (last visited Jan. 31, 2024).
[10] Caitlyn Stroh-Page, TALLAHASSEE DEMOCRAT, *Social Security Numbers, Some Patient Treatment Info Involved in TMH Cybersecurity Incident* (Apr. 1, 2023) https://www.tallahassee.com/story/news/local/2023/03/31/tmh-updates-what-information-was-affected-during-cybersecurity-incident/70069655007/ (last visited Jan. 25, 2024).
[11] The term "information technology" means equipment, hardware, software, firmware, programs, systems, networks, infrastructure, media, and related material used to automatically, electronically, and wirelessly collect, receive, access, transmit, display, store, record, retrieve, analyze, evaluate, process, classify, manipulate, manage, assimilate, control, communicate, exchange, convert, converge, interface, switch, or disseminate information of any kind or form. Section 282.0041(19), F.S.
[12] *See* s. 20.22, F.S.
[13] Chapter 2020-161, Laws of Fla.
[14] *See* s. 20.22(2)(b), F.S.
[15] The Secretary of Management Services serves as the head of the DMS and is appointed by the Governor, subject to confirmation by the Senate. Section 20.22(1), F.S.
[16] Section 282.0051(2)(a), F.S.
[17] *Id*.
[18] Section 282.0051(1), F.S.
[19] *Id*.

- Provide oversight for 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;[20] and
- Standardize and consolidate IT services that support interoperability, Florida's cloud first policy, and business functions and operations that are common across state agencies.

State Cybersecurity Act

While it has existed in some form for more than 10 years, in 2022, the Legislature passed the State Cybersecurity Act,[21] which requires the DMS and the heads of the state agencies[22] to meet certain requirements to enhance the cybersecurity[23] of the state agencies.

The DMS through FLDS is tasked with completing the following:[24]

- Establish standards for assessing agency cybersecurity risks;
- Adopt rules to mitigate risk, support a security governance framework, and safeguard agency digital assets, data,[25] information, and IT resources;[26]
- Designate a chief information security officer (CISO);
- Develop and annually update a statewide cybersecurity strategic plan such as identification and mitigation of risk, protections against threats, and tactical risk detection for cyber incidents;[27]
- Develop and publish for use by state agencies a cybersecurity governance framework;
- Assist the state agencies in complying with the State Cybersecurity Act;
- Provide annual training on cybersecurity for information security managers and computer security incident response team members;
- Annually review the strategic and operational cybersecurity plans of state agencies;
- Track the 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;
- Maintain a Cybersecurity Operations Center (CSOC) led by the CISO to serve as a clearinghouse for threat information and coordinate with the FDLE to support responses to incidents; and
- Lead an Emergency Support Function under the state emergency management plan.

[20] The FLDS provides project oversight on IT projects that have a total cost of $20 million or more for the Department of Financial Services, the Department of Legal Affairs, and the Department of Agriculture and Consumer Services. Section 282.0051(1)(m), F.S.
[21] Section 282.318, F.S.
[22] For purposes of the State Cybersecurity Act, the term "state agency" includes the Department of Legal Affairs, the Department of Agriculture and Consumer Services, and the Department of Financial Services. Section 282.318(2), F.S.
[23] "Cybersecurity" means the protection afforded to an automated information system in order to attain the applicable objectives of preserving the confidentiality, integrity, and availability of data, information, and information technology resources. Section 282.0041(8), F.S.
[24] Section 282.318(3), F.S.
[25] "Data" means a subset of structured information in a format that allows such information to be electronically retrieved and transmitted. Section 282.0041(9), F.S.
[26] "Information technology resources" means data processing hardware and software and services, communications, supplies, personnel, facility resources, maintenance, and training. Section 282.0041(22), F.S.
[27] "Incident" means a violation or imminent threat of violation, whether such violation is accidental or deliberate, of information technology resources, security, policies, or practices. An imminent threat of violation refers to a situation in which the state agency has a factual basis for believing that a specific incident is about to occur. Section 282.0041(19), F.S.

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.[28] The head of the agency has additional tasks in protecting against cybersecurity threats as follows:[29]

- Establish a cybersecurity incident response team with the FLDS and the Cybercrime Office, which must immediately report all confirmed or suspected incidents to the CISO;
- Annually submit to the DMS the state agency's strategic and operational cybersecurity plans;
- Conduct and update a comprehensive risk assessment to determine the security threats once every three years;
- 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)[30] cybersecurity framework;
- Provide cybersecurity training to all agency employees within 30 days of employment;
- Develop a process that is consistent with the rules and guidelines established by the FLDS for detecting, reporting, and responding to threats, breaches, or cybersecurity incidents; and
- Submit an after-action report to the FLDS within one week after remediation of a cybersecurity incident or ransomware incident.

Florida Cybersecurity Advisory Council

The Florida Cybersecurity Advisory Council[31] (CAC) within the DMS[32] assists state agencies in protecting IT resources from cyber threats and incidents.[33] The CAC must assist the 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.[34] The CAC meets at least quarterly to:[35]

- 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;

[28] Section 282.318(4)(a), F.S.
[29] Section 282.318(4), F.S.
[30] 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 (May. 6, 2023), https://www.digitalguardian.com/blog/what-nist-compliance (last visited Jan. 31, 2024).
[31] Under Florida law, an "advisory council" means an advisory body created by specific statutory enactment and appointed to function on a continuing basis. 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. Section 20.03(7), F.S.; *See also* s. 20.052, F.S.
[32] Section 282.319(1), F.S.
[33] Section 282.319(2), F.S.
[34] Section 282.319(2)-(3), F.S.
[35] Section 282.319(9), F.S.

- Assist the FLDS in developing cybersecurity best practice recommendations; and
- Examine inconsistencies between state and federal law regarding cybersecurity.

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.[36]

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 as stated below:[37]

- 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 by the U.S. Department of Homeland Security, according to the direction of Presidential Policy Directive (PPD)-41.[38] 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.[39] The NCIRP was developed in coordination with federal, state, local, and private sector entities and is designed to interface with industry best practice standards for cybersecurity, including the NIST Cybersecurity Framework.

The NCIRP adopted a common schema for describing the severity of cybersecurity incidents affecting the U.S. The schema establishes a common framework to evaluate and assess cybersecurity incidents to ensure that all departments and agencies have a common view of the severity of a given incident; urgency required for responding to a given incident; seniority level

[36] Section 282.319(10), F.S.
[37] Section 282.319(11), F.S.
[38] Annex for PPD-41: *U.S. Cyber Incident Coordination*, https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/annex-presidential-policy-directive-united-states-cyber-incident (last visited Jan. 31, 2024).
[39] Cybersecurity & Infrastructure Security Agency, *Cybersecurity Incident Response*, 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. 31, 2024).

necessary for coordinating response efforts; and level of investment required for response efforts.[40]

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.
- 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.[41]

State agencies and local governments in Florida, must report to the CSOC all ransomware incidents and any cybersecurity incidents at severity levels of three, four, or five as soon as possible, but no later than 48 hours after discovery of a cybersecurity incident and no later than 12 hours after discovery of a ransomware incident.[42] The CSOC is required to notify the President of the Senate and the Speaker of the House of Representatives of any incidents at severity levels of three, four, or five as soon as possible, but no later than 12 hours after receiving the incident report from the state agency or local government.[43] For state agency incidents at severity levels one and two, they must report these to the CSOC and the Cybercrime Office at the FDLE as soon as possible.[44]

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

[40] *Id.*
[41] Section 282.318(3)(c)9.a, F.S.
[42] Sections 282.318(3)(c)9.c(I), F.S. and 282.3185(5)(b)1., F.S.
[43] Section 282.318(3)(c)9.c.(II), F.S.
[44] Section 282.318(3)(c)(9)(d), F.S.

- If the reporting entity is a local government, a statement requesting or declining assistance from the CSOC, FDLE Cybercrime Office, or sheriff.[45]

In addition, the 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.[46] 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.[47]

State agencies and local governments must submit an after-action report to the FLDS within one week of the remediation of a cybersecurity or ransomware incident.[48] The report must summarize the incident, state the resolution, and any insights from the incident.

Public Record and Public Meetings Exemption for Specific Cybersecurity Records Held by Agencies

The State Cybersecurity Act makes confidential and exempt from public records copying and inspection requirements the portions of risk assessments, evaluations, external audits, and other agency cybersecurity program reports that are held by an agency, if the disclosure would facilitate unauthorized access to, modification, disclosure, or destruction of data or IT resources.[49] However, this information must be shared with the Auditor General, DLE Cybercrime Office, FLDS, and the Chief Inspector General. An agency may share its confidential and exempt documents with a local government, another agency, or a federal agency if given for a cybersecurity purpose, or in furtherance of the agency's official duties.[50] Additionally, any document that, when held by an agency, is exempt or confidential and exempt under s. 119.07(1), F.S., maintains its exempt status when the custodian agency shares it with the legislature.[51]

The State Cybersecurity Act also exempts portions of any public meeting that would reveal records that it makes confidential and exempt.[52]

Florida Fusion Center

To help unify the Nation's efforts to share information and exchange intelligence, the Intelligence Reform and Terrorism Prevention Act of 2004 (Act) was passed. The Act provides guidance to agencies at all levels about information sharing, access and collaboration. Part of this guidance is the need to designate a single fusion center in each state to serve as the "hub" for these activities.[53]

[45] Section 282.318(3)(c)9.b, F.S.
[46] Section 282.318(3)(c)9.e, F.S.
[47] *Id*.
[48] Section 282.318(4)(k), F.S.
[49] Section 282.318(5), F.S.
[50] Section 282.318(7), F.S.
[51] Section 11.0431(2)(a), F.S.
[52] Section 282.318(6), F.S.
[53] Florida Department of Law Enforcement, *Florida Fusion Center History*, https://www.fdle.state.fl.us/FFC/FusionCenterHistory (last visited January 31, 2024).

The Florida Fusion Center (FFC) began operations in 2007 and is located in Tallahassee, Florida. The FFC was designated as the state's primary fusion center by the Governor in March of 2008 and serves as the head of the Network of Florida Fusion Centers. There are regional fusion centers in each of the seven FDLE regions to support local and state intelligence needs. [54]

The FFC provides connectivity and coordinates intelligence sharing among seven regional fusion centers located throughout the state. Operations are guided by the understanding that the key to effectiveness is the development and sharing of information to the fullest extent permitted by law and agency policy. The FFC consists of approximately 45 FDLE members, federal agencies, and 12 multi-disciplinary state agency partners; and includes outreach to private sector entities.[55]

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.[56] The goals of Cyber Florida are to:[57]

- 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.

III. Effect of Proposed Changes:

Technology Services Contract Restrictions

Section 1 prohibits the state, any special district, or any municipal subdivision from awarding a contract to a vendor that has shared security information with companies or individuals in non-TAA compliant nations without prior written consent.

Florida Center for Cybersecurity

Section 2 provides that the Florida Center for Cybersecurity may also be referred to as "Cyber Florida." The bill clarifies that Cyber Florida operates under the discretion of the University of South Florida's (USF) president or designee. The USF president may assign, with the USF board

[54] *Id*.
[55] Florida Department of Law Enforcement, *Long-Range Program Plan Fiscal Years 2010-2011 through 2014-2015, September 30, 2009*, available at http://floridafiscalportal.state.fl.us/Document.aspx?ID=2215&DocType=PDF (last visited Jan. 31, 2024).
[56] Section 282.318(4)(k), F.S.
[57] Section 1004.444, F.S.

of trustee's approval, Cyber Florida to a college within USF that has a strong emphasis on cybersecurity, technology, or computer sciences and engineering.

The bill allows Cyber Florida, at the request of the DMS, FLDS, or other state agency, to assist any state-funded initiatives that relate to: (1) cybersecurity training, professional development, and education for state and local government employees, and (2) increasing the cybersecurity effectiveness of the state and local government technology platforms and infrastructure.

The bill also clarifies the mission and goals of Cyber Florida.

Enterprise Cybersecurity Resiliency Program Oversight

Section 3 instructs the Department of Management Services to contract with an independent verification and validation (IV&V) provider to provide program oversight for the Enterprise Cybersecurity Resiliency Program. It further requires the IV&V vendor to complete a program assessment and provide recommendations to the legislature and Office of Policy and Budget by December 1, 2024, based on specific evaluation criteria.

Section 4 provides that the bill takes effect July 1, 2024.

IV. Constitutional Issues:

A. Municipality/County Mandates Restrictions:

Not applicable. 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:

The provision added in Section 1 of the bill implicates the following constitutional issues:

Retroactive Application

The State cannot retroactively increase a penalty for past conduct.[58] Absent an express statement of legislative intent, a statute is presumed to operate only prospectively, not retroactively.[59] The bill applies a penalty (prohibition on bidding and contracting with the state) for activity that may have occurred 7 years prior to its effective date; this may be found to constitute an increased penalty for past conduct.

Foreign CommerceArticle I, section 8 of the United States Constitution grants Congress the power to "regulate Commerce with foreign Nations[.]" This power is Congress' exclusive domain, in which states have even less freedom to act than with respect to the regulation of interstate commerce.[60] Courts hold state or local laws to unconstitutionally conflict with the Congressional foreign commerce power if they impair the federal government's ability to speak with "one voice" internationally.[61] In those cases where state or local laws with international effect have been found valid, this has usually been because Congress had an opportunity to examine the specific issue and either acquiesced in, or affirmatively granted, the states' authority to do so.[62] In determining compliance with this factor, international agreements regulating trade are relevant.

The bill's prohibition on sharing information with firms in foreign countries may prevent the federal government from "speaking with one voice" when regulating commercial relations with foreign governments.

Due Process

It is not clear what entity must making a finding of a violation that disqualifies a firm from Florida state contracting for 7 years, or what evidentiary standard applies to that finding. This may result in an arbitrary application of the law in violation of the firm's due process right to contract and right to engage in an occupation.[63] The 14th amendment of U.S. Constitution, as it applies to the states, requires that states provide due process of law before it can deprive any person of life, liberty, or property. Generally, due process requires in any proceeding which is to be accorded finality reasonable notice which apprises interested parties of the pendency of the action and which affords them an opportunity to present their objection.[64]

Non-Delegation Doctrine

The Legislature may not delegate the power to enact a law, to declare what the law must be, or to exercise an unrestricted discretion in applying the law. Specifically, the adoption by the Legislature in advance of any federal act or the ruling of any federal administrative

[58] *Calder v. Bull*, 3 U.S. 386 (1978); *see Stogner v. California*, 539 U.S. 607 (2003).
[59] *Fla. Ins. Guar. Ass'n, Inc. v. Devon Neighborhood Ass'n, Inc.*, 67 So. 3d 187, 194-95 (Fla. 2011).
[60] *See, Michelin Tire Corp. v. Wages*, 423 U.S. 276 (1976).
[61] *Barclays Bank PLC v. Franchise Tax Board*, 512 U.S. 298, 328 (1994).
[62] *See Id.*; *Wardair Canada v. Fla. Dept. of Rev.*, 477 U.S. 1 (1986); *Gerling Global Reinsurance* 267 F.3d 1228, 1237 (11th Cir. 2001).
[63] *Bd. of Regents of State Colls. v. Roth*, 408 U.S. 564 (1972).
[64] *Mullane v. Central Hanover Bank & Trust Co.*, 339 U.S. 306, 314 (1950).

body, as Congress or such administrative body might see fit to adopt in the future, constitutes an unconstitutional delegation of legislative power.[65] The bill's reliance of the United States Trade Agreements Act list of compliant nations may constitute a delegation of Legislative authority.

V. Fiscal Impact Statement:

A. Tax/Fee Issues:

None.

B. Private Sector Impact:

None.

C. Government Sector Impact:

None.

VI. Technical Deficiencies:

None.

VII. Related Issues:

The language does not define the term "share". It is unclear if a security breech that resulted in the release of data to a non-TAA compliant nation would disqualify a vendor from contracting with the state. The language also does not describe how a disqualifying sharing event would be validated.

VIII. Statutes Affected:

This bill substantially amends section 1004.444 of the Florida Statutes.

IX. Additional Information:

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

CS/CS/CS by Appropriations on February 27, 2024:
The committee substitute adds a section prohibiting a contract award to technology services vendors that have shared information with non-United States Trade Agreements Act complaint nations without prior written consent within the past 7 years.

CS/CS by Appropriations Committee on Agriculture, Environment, and General Government on February 20, 2024:
The committee substitute:

[65] *State Dept. of Children and Family Servs. v. L.G.*, 801 So. 2d 1047 (Fla. 1st DCA 2001); *State v. Carswell*, 557 So. 2d 183 (Fla. 3d DCA 1990); *Florida Citrus Processors Ass'n. v. Jesse J. Parrish, Inc.*, 415 So. 2d 1299 (Fla. 2d DCA 1982).

- Removes all statutory revisions related to the Florida Digital Service.
- Requires the Department of Management Services to contract with an independent verification and validation provider to provide program oversight and an assessment of the Enterprise Cybersecurity Resiliency program**.**

CS by Governmental Oversight and Accountability on January 29, 2024:

- Removes provisions of the bill that designate certain information security personnel positions as selected exempt positions.
- Removes provisions of the bill that require each state agency head to designate a chief information security officer that reports to the Florida Digital Services' (FLDS) chief information officer, and instead amends the role of the currently-serving agency information security manager to "ensure compliance with cybersecurity governance and with the state's enterprise security program and incident response plan." This amendment also requires the agency information security manager to coordinate with information security personnel within his or her agency and the Cybersecurity Operations Center within the FLDS.
- Updates the mission, goals, and responsibilities of the Florida Center for Cybersecurity ("Cyber Florida") housed within University of South Florida (USF), and authorizes the USF president to assign the Center to an appropriate college within the university, with approval of the board of trustees.

B. Amendments:

None.