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:	SB 2508
INTRODUCER:	Appropriations Committee
SUBJECT:	State Cybersecurity Operations
DATE:	March 29, 2023
REVISED:	

ANALYST	STAFF DIRECTOR	REFERENCE	ACTION
Hunter	Sadberry		**AP Submitted as Comm. Bill/Fav**

I. Summary:

SB 2508 transfers the Cybersecurity Operations Center (CSOC) and its associated duties, responsibilities, contracts, unexpended balances of appropriations, allocations, and positions from the Florida Digital Service (FDS) within the Department of Management Services (DMS) to the Florida Department of Law Enforcement (FDLE) via a type two transfer. The FDS maintains primary responsibility for establishing enterprise cybersecurity policies and guidelines in consultation with the state chief information security officer. The FDS is also tasked with assessing and monitoring agency compliance with the cybersecurity governance framework. In accordance with the recommendations of the February 1, 2021, Florida Cybersecurity Task Force Final Report, the bill also requires state agencies to conduct comprehensive risk assessments on an annual basis instead of once every three years.

The bill takes effect July 1, 2023.

II. Present Situation:

Over the last decade, cybersecurity has rapidly become a growing concern. The cyberattacks are growing in frequency and severity. Cybercrime is 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

[1] Cybercrime Magazine, *Cybercrime to Cost the World $8 Trillion Annually in 2023,* Cybercrime To Cost The World 8 Trillion Annually In 2023 (cybersecurityventures.com) (last visited March 21, 2023).

[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 March 21, 2023).

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 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. 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 February 2023, and the hospital's systems were forced to shut down, impacting many local residents in need of medical care.[7]

Information Technology and Cybersecurity Management

The Department of Management Services (DMS) oversees information technology (IT)[8] governance and security for the executive branch in Florida.[9] The Florida Digital Service (FDS) is housed within the DMS and was established in 2020 to replace the Division of State Technology.[10] The FDS works under the DMS to implement policies for information technology and cybersecurity for state agencies.[11]

The head of the FDS is appointed by the Secretary of Management Services[12] and serves as the state chief information officer (CIO).[13] The CIO must have at least five years of experience in

---

[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 March 21, 2023).
[5] "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 March 21, 2023).
[6] Cybersecurity and Infrastructure Agency, *Ransomware 101*, https://www.cisa.gov/stopransomware/ransomware-101 (last visited March 21, 2023).
[7] Tallahassee Democrat, *TMH says it has taken 'major step' toward restoration after cybersecurity incident* (February 15, 2023) https://www.tallahassee.com/story/news/local/2023/02/14/tmh-update-hospital-has-taken-major-step-toward-restoration/69904510007/ (last visited March 21, 2023).
[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] *See* s. 20.22, F.S.
[10] Chapter 2020-161, L.O.F.
[11] *See* s. 20.22(2)(b), F.S.
[12] 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.
[13] Section 282.0051(2)(a), F.S.

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.[14] The FDS 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.[15]

The DMS, through the 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; 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.[16]

Information Technology Security Act

In 2021, the Legislature passed the IT Security Act,[17] which requires the DMS and the state agency[18] heads to meet certain requirements in order to enhance the IT security of state agencies. Specifically, the IT Security Act provides that the DMS is responsible for establishing standards and processes consistent with accepted best practices for IT security,[19] including cybersecurity, and adopting rules that help agencies safeguard their data, information, and IT resources to ensure availability, confidentiality, integrity, and to mitigate risks.[20] In addition, the 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 governance framework for use by state agencies;
- Collaborate with the Cybercrime Office within the Florida Department of Law Enforcement (FDLE) to provide training; and
- Annually review the strategic and operational IT security plans of executive branch agencies.[21]

[14] *Id.*
[15] Section 282.0051 (1), F.S.
[16] *Id.*
[17] Section 282.318, F.S.
[18] 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. S. 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.
[19] 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.
[20] Section 292.318(3), F.S.
[21] *Id.*

State Cybersecurity Act

In 2022, the Legislature passed the State Cybersecurity Act,[22] which requires the DMS and the heads of the state agencies[23] to meet certain requirements to enhance the cybersecurity[24] of the state agencies.

The DMS through FDS is tasked with completing the following:

- Establishing standards for assessing agency cybersecurity risks;
- Adopting rules to mitigate risk, support a security governance framework, and safeguard agency digital assets, data,[25] information, and IT resources;[26]
- Designating a chief information security officer (CISO);
- Developing and annually updating a statewide cybersecurity strategic plan such as identification and mitigation of risk, protections against threats, and tactical risk detection for cyber incidents;[27]
- Developing and publishing for use by state agencies a cybersecurity governance framework;
- Assisting the state agencies in complying with the State Cybersecurity Act;
- Annually providing training on cybersecurity for managers and team members;
- Annually reviewing the strategic and operational cybersecurity plans of state agencies;
- Tracking the state agencies' implementation of remediation plans;
- Providing cybersecurity training to all state agency technology professionals that develops, assesses, and documents competencies by role and skill level;
- Maintaining a Cybersecurity Operations Center (CSOC) led by the CISO to serve as a clearinghouse for threat information and coordinate with the FDLE to support responses to incidents; and
- Leading an Emergency Support Function under the state emergency management plan.[28]

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

- 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;

[22] Section 282.318, F.S.
[23] 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.
[24] "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.
[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.
[28] Section 282.318(3), F.S.
[29] Section 282.318(4)(a), F.S.

- 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; and
- Develop a process that is consistent with the rules and guidelines established by the FDS for detecting, reporting, and responding to threats, breaches, or cybersecurity incidents.[31]

Florida Cybersecurity Advisory Council

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

- Review existing state agency cybersecurity policies;
- Assess ongoing risks to state agency IT;
- Recommend a reporting and information sharing system to notify state agencies of new risks;
- Recommend data breach simulation exercises;
- Assist the FDS in developing cybersecurity best practice recommendations; and
- Examine inconsistencies between state and federal law regarding cybersecurity.[36]

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.[37]

---

[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 (Dec. 1, 2020), https://www.digitalguardian.com/blog/what-nist-compliance (last visited March 17, 2023).
[31] Section 282.318(4), F.S.
[32] 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.
[33] Section 282.319(1), F.S.
[34] Section 282.319(2), F.S.
[35] Section 282.319(3), F.S.
[36] Section 282.319(9), F.S.
[37] Section 282.319(10), F.S.

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:

- Descriptive statistics, including the amount of ransom requested, duration of the incident, and overall monetary cost to taxpayers of the incident;
- A detailed statistical analysis of the circumstances that led to the ransomware incident which does not include the name of the state agency or local government, network information, or system identifying information;
- Statistical analysis of the level of cybersecurity employee training and frequency of data backup for the state agencies or local governments that reported incidents;
- Specific issues identified with current policy, procedure, rule, or statute and recommendations to address those issues; and
- Other recommendations to prevent ransomware incidents.

Cyber Incident Response

The National Cyber Incident Response Plan (NCIRP) was developed according to the direction of Presidential Policy Directive (PPD)-41,[38] by the U.S. Department of Homeland Security. The NCIRP is part of the broader National Preparedness System and establishes the strategic framework for a whole-of-Nation approach to mitigating, responding to, and recovering from cybersecurity incidents posing risk to critical infrastructure.[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 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.

[38] Annex for PPD-41: *U.S. Cyber Incident Coordination*, available at: https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/annex-presidential-policy-directive-united-states-cyber-incident (last visited March 15, 2023).
[39] Cybersecurity & Infrastructure Security Agency, *Cybersecurity Incident Response*, available at https://www.cisa.gov/topics/cybersecurity-best-practices/organizations-and-cyber-safety/cybersecurity-incident-response#:~:text=%20National%20Cyber%20Incident%20Response%20Plan%20%28NCIRP%29%20The,incidents%20and%20how%20those%20activities%20all%20fit%20together (last visited March 15, 2023).
[40] *Id.*

- 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 Cybersecurity Operations Center (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
- 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]

Legislation passed in 2022 required state agencies and local governments to submit an after-action report to the FDS within one week of the remediation of a cybersecurity or ransomware

[41] Section 282.318(3)(c)9.a, F.S.
[42] Section 282.318(3)(c)9.a, F.S.
[43] Section 282.318(3)(c)9.c.(II), F.S.
[44] Section 282.318(3)(c)(9)(d), F.S.
[45] Section 282.318(3)(c)9.b, F.S.
[46] Section 282.318(3)(c)9.e, F.S.
[47] *Id*.

incident.[48] The report must summarize the incident, state the resolution, and any insights from the incident.

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.[49]

The Florida Fusion Center, also known as 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. [50]

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 twelve multi-disciplinary state agency partners; and includes outreach to private sector entities.[51]

III. Effect of Proposed Changes:

The bill transfers by a type two transfer all positions, duties, functions, records, existing contracts, administrative authority, administrative rules, and unexpended balances of appropriations, allocations, and other public funds related to the Cybersecurity Operations Center (CSOC) and enterprise cybersecurity resiliency from the Florida Digital Service (FDS) within the Department of Management Services (DMS) to the Department of Law Enforcement (FDLE). The transfer includes the State Chief Information Security Officer position.

Florida Digital Service

The DMS, acting through the FDS, maintains the designation as the lead entity responsible for establishing standards and processes for assessing state agency cybersecurity risks. However, the bill removes the lead entity designation for the responsibility of determining appropriate security measures.

---

[48] Section 282.318(4)(k), F.S.
[49] Florida Department of Law Enforcement, *Florida Fusion Center History*, *available at* https://www.fdle.state.fl.us/FFC/FusionCenterHistory (last visited March 21, 2023).
[50] *Id.*
[51] 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 March 21, 2023).

The bill requires the FDS to assess agency compliance with the cybersecurity governance framework. Specifically, the bill amends s. 282.318, F.S., to require the DMS, acting through the FDS to:

- Assist state agencies in complying with s. 282.318, F.S.
- Annually review agency strategic and operational cybersecurity plans for compliance with the cybersecurity governance framework pursuant to the following requirements:
  - Provide findings to the state chief information security officer for review confirmation
  - Notify agencies of confirmed findings and the date by which the agency must submit a corrective action plan;
  - Review corrective action plans submitted by agencies;
  - Track and monitor progress of the implementation of corrective action plans; and
  - Submit an annual report to the state chief information security officer, which includes, by agency, completed reviews, any confirmed findings, corresponding corrective action plans, and the status of corrective action plan implementation.
- Review state agency annual risk assessment findings and corresponding remediation plans, including:
  - Tracking and monitoring the progress of the risk assessment remediation plans; and
  - Submit an annual report to the state chief information security officer, which includes, by agency, risk assessment findings, corresponding remediation plans, and the status of remediation plan implementation.
- Provide annual cybersecurity training that includes cybersecurity threats, trends, and best practices, for state agency information security managers and computer security incident response team members. The training curriculum must be approved by the state chief information security officer.
- Provide annual cybersecurity training to all state agency technology professionals and employees with access to highly sensitive information. The training curriculum must include training on the identification of each cybersecurity incident severity level

The FDS is also tasked with reviewing, tracking, and reporting state agency risk assessment findings, remediation plans, and remediation progress to the state chief information security officer.

While the cybersecurity governance framework and cybersecurity training will continue to be developed and provided to agencies and local governments by the FDS, s. 282.3185, F.S., is amended to require the state chief information security officer to coordinate with the FDS and approve the cybersecurity governance framework and training curriculum. The bill also removes the incident response reporting process from the cybersecurity governance framework.

Florida Department of Law Enforcement

The FDLE is designated as the lead entity responsible for enterprise security operations. The responsibilities associated with said designation include:

- Selecting an employee to serve as the state chief information security officer;
- Reporting all confirmed or suspected incidents or threats of state agency information technology resources to the state chief information officer and the Governor;
- Developing and annually updating a statewide cybersecurity strategic plan;

- Operating and maintaining a cybersecurity operations center;
- Coordinating with FDS to support state agencies;
- Reviewing and approving all enterprise cybersecurity training; and
- Developing and publishing a cybersecurity incident reporting process that includes procedures and secure communication mechanisms.

State Agencies

Provisions within the bill require state agencies to coordinate with the FDLE and to submit to the FDS:

- Corrective action plans for confirmed findings related to non-compliance with the cybersecurity governance framework within 90 days of notification; and
- Quarterly status reports on the implementation of corrective action plans until fully resolved.

The bill also addresses a recommendation in the February 1, 2021, Florida Cybersecurity Task Force Final Report, by requiring agencies to conduct comprehensive risk assessments on an annual basis instead of once every three years.

IV. Constitutional Issues:

A. Municipality/County Mandates Restrictions:

None.

B. Public Records/Open Meetings Issues:

None.

C. Trust Funds Restrictions:

None.

D. State Tax or Fee Increases:

None.

E. Other Constitutional Issues:

None.

V. Fiscal Impact Statement:

A. Tax/Fee Issues:

None.

B. Private Sector Impact:

None.

C. Government Sector Impact:

This bill transfers the Cybersecurity Operations Center and its associated duties, responsibilities, contracts, unexpended balances of appropriations, allocations, and positions from the Florida Digital Service within the Department of Management Services to the Florida Department of Law Enforcement (FDLE) via a type two transfer.

VI. Technical Deficiencies:

None.

VII. Related Issues:

None.

VIII. Statutes Affected:

This bill substantially amends the following sections of the Florida Statuts: 282.318 and 282.3185.

IX. Additional Information:

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

None.

B. Amendments:

None.