HOUSE OF REPRESENTATIVES
FINAL BILL ANALYSIS

BILL #:	HB 5301	**FINAL HOUSE FLOOR ACTION:**	
SUBJECT/SHORT TITLE	Information Technology Reorganization	109 **Y's**	2 **N's**
SPONSOR(S):	Ingoglia	**GOVERNOR'S ACTION:**	Vetoed
COMPANION BILLS:	N/A		

SUMMARY ANALYSIS

House Bill 5301 passed the House on May 8, 2017, as amended by the conference committee. The Senate concurred in the conference committee amendment to the House Bill and subsequently passed the Bill as amended on May 8, 2017.

The bill revises the structure and responsibilities of the Agency for State Technology (AST). Specifically, the bill:

- Removes from statute the deputy executive director, chief planning officer, chief operations officer, and chief technology officer.
- Revises the qualifications for the state CIO by requiring at least 10 years of executive-level experience in either the public or private sector, with experience in the development of information technology strategic planning and the development and implementation of fiscal and substantive information technology policy and standards.
- Revises the project oversight duties and responsibilities of the AST to include:
    - Reviewing state agency project oversight deliverables on IT projects with total costs of $10 million or more,
    - Reviewing project oversight deliverables on cabinet agency IT projects that have a total project cost of $25 million or more and impact another agency or agencies,
    - Recommending improvements for state agency and cabinet agency IT projects and project oversight,
- Requires the State Chief Information Officer (CIO) to recommend best practices for the procurement of cloud computing services.
- Removes the responsibility of the AST to review state agency technology purchases over $250,000.
- Provides for the cost recovery of AST executive direction through charges to state data center customer entities.
- Deletes legislative intent language for data center consolidation and the obsolete consolidation schedule.
- Requires the State Data Center and state agency customer entities to utilize cloud computing services when beneficial use of these services is validated through cost benefit analyses.
- Creates the Florida Cybersecurity Task Force to review and provide recommendations for the improvement of the state's cybersecurity infrastructure, governance, and operations.
- Conforms to the conference report for Senate Bill 2500 General Appropriations Act (GAA) - the positions removed from statute have no funding in the budget except for the chief operations officer, which will be reclassified as the state data center director.
    - Appropriates a total of $100,000 to the Florida Department of Law Enforcement for support of the Florida Cybersecurity Task Force.

The effective date of this bill was July 1, 2017; however, this bill was vetoed by the Governor on June 26, 2017.

I. SUBSTANTIVE INFORMATION

A. EFFECT OF CHANGES:

Agency for State Technology Duties and Responsibilities

Current Situation

In 2014, the Legislature created the Agency for State Technology to oversee policies for the design, planning, project management, and implementation of enterprise IT services[1].

The AST is headed by an executive director who serves as the state's chief information officer and is appointed by the Governor and confirmed by the Senate. Current law requires that the state CIO preferably have executive-level experience in both the public and private sectors in development and implementation of information technology strategic planning; management of enterprise information technology projects, particularly management of large-scale consolidation projects; and development and implementation of fiscal and substantive information technology policy.

Duties and responsibilities of the AST include:[2]

- developing and implementing IT architecture standards,
- implementing industry standards and best practices for the state data center,
- establishing project management and oversight standards,
- performing project oversight on IT projects with total costs of $10 million or more,
- providing operational management and oversight of the State Data Center,
- reviewing IT purchases over $250,000 made by state agencies,
- identifying opportunities for standardization and consolidation of IT services that support common business functions,
- recommending additional consolidations of agency data centers or computing facilities, and
- Performing project oversight on any cabinet agency IT project that has a total project cost of $25 million or more and impacts another agency or agencies.

Effect of Changes

The bill revises the structure of the Agency for State Technology (AST) and the qualifications of the state CIO. Specifically, the bill:

- removes from statute the deputy executive director, chief planning officer, chief operations officer, and chief technology officer.
- revises the qualifications for the state CIO by requiring at least 10 years of executive-level experience in either the public or private sector, with experience in the development of information technology strategic planning and the development and implementation of fiscal and substantive information technology policy and standards.

The bill revises the duties and responsibilities to include:

- reviewing state agency project oversight deliverables on IT projects with total costs of $10 million or more,
- reviewing project oversight deliverables on cabinet agency IT projects that have a total project cost of $25 million or more and impact another agency or agencies,
- recommending improvements for state agency and cabinet agency IT projects and project oversight,
- recommending best practices for the procurement of cloud computing services, and

[1] 2014-221, Laws of Florida.
[2] Section 282.0051, Florida Statutes.

- removing the responsibility of the AST to review state agency technology purchases over $250,000.

The bill also amends the section of law defining the duties of the cabinet agencies[3] by requiring cabinet agencies by January 1, 2018, to submit project oversight deliverables to the AST for all IT projects with a total project cost of $25 million or more and that impact one or more other agencies.

The State Data Center

Current Situation

In 2014, the Legislature merged two existing primary state data centers to create the State Data Center, established within the AST, to provide data center services that are hosted either on premises or externally through a third-party provider[4]. The data center director is appointed by the AST executive director. The State Data Center must comply with all applicable state and federal laws, regulations and policies. The State Data Center's duties include:

- Entering into service level agreements with each customer entity.
- Developing and implementing a business continuity plan and a disaster recovery plan and annually conducting a live exercise of each plan.
- Maintaining the performance of the State Data Center.
- For purposes of chapter 273, being the custodian of resources and equipment consolidated and located within the State Data Center.
- Assuming administrative access rights to resources and equipment consolidated into the State Data Center.

Section 282.0051, F.S. requires the AST to establish a consolidated administrative support structure that is responsible for the provision of financial management, procurement, transactions involving real or personal property, human resources, and operational support for the State Data Center.

Section 282.0051, F.S. requires that the AST develop and implement cost-recovery mechanisms that recover the full direct and indirect cost of services through charges to applicable customer entities. Current statute allows only data center services to be cost-recovered.

Effect of Changes

The bill amends s. 282.201, F.S., requiring the AST executive director to appoint a State Data Center director who has experience in leading data center facilities and cloud computing management.

The bill amends definitions in 282.0041, F.S. to allow for the cost recovery of AST executive direction through charges to state data center customer entities.

The State Data Center duties include:

- Developing and implementing appropriate operating guidelines and procedures necessary for the State Data Center to perform its duties.
- Entering into service level agreements with each customer entity.
- Developing and implementing a business continuity plan and a disaster recovery plan and annually conducting a live exercise of each plan.
- Maintaining the performance of the State Data Center.
- For purposes of chapter 273, being the custodian of resources and equipment consolidated and located within the State Data Center.
- Assuming administrative access rights to resources and equipment consolidated into the State Data Center.

[3] Section 282.00515, Florida Statutes.
[4] Section 282.201, Florida Statutes.

The bill also amends s. 282.201, F.S., defining the duties of the State Data Center by requiring use of cloud computing services when beneficial use of these services is validated through cost benefit analyses. Additionally, the bill requires the State Data Center to report biennially on the use of cloud computing by state agency customer entities.

The bill creates a new section of law defining the duties of state agency customer entities. Duties of state agency customer entities include:

- Notifying the State Data Center, by May 31 and November 30 of each year, of any significant changes in anticipated usage of State Data Center services.
- Developing a plan updated annually to address its software applications located at the State Data Center. The plan includes the following components:
  - An inventory of the agency's applications at the state data center.
  - For each application that may begin migration activities:
    - the recommended strategy for migration to a third party cloud computing service provider,
    - a proposed project and budget estimate for the migration project, and
    - a cost benefit analysis validating that a cloud computing service can reduce customer entity data center costs, deliver the same or improved levels of service, and meet or exceed the applicable state and federal standards for IT security.
- Utilizing a cloud computing service when developing, upgrading, or purchasing software, when a cost benefit analysis confirms that a cloud computing service can deliver the same or improved levels of service, and meet or exceed the applicable state and federal standards for IT security.

Agency Data Center Consolidations

Current Situation

In 2012, the Legislature amended the agency data center consolidation schedule and provided an exemption from data center consolidation to certain agencies.[5] Additionally, the Implementing Bill for the Fiscal Year 2013-2014 General Appropriations Act[6] modified the data center consolidation schedule in s. 282.201(4), F.S.

Agencies scheduled for consolidation are required to submit a transition plan to the data center by July 1 of the fiscal year before the fiscal year the scheduled consolidation will occur. State agencies are required to execute a new or update an existing service-level agreement within 60 days after the specified consolidation date.

All agencies that were required to consolidate into the State Data Center completed their consolidation activities by the dates specified in law.

Effect of Changes

The bill amends s. 282.201, F.S. by removing subsections (1) and (4) that establish the legislative intent for data center consolidation and the schedule for consolidations of agency data centers.

Information Technology Security

Current Situation

[5] 2012-142, Laws of Florida.
[6] 2013-41, Laws of Florida.

Section 282.318, F.S. establishes the requirements for the security of data and information technology. The AST's duties in regards to IT security include:

- Establishing standards and processes for IT security consistent with generally accepted best practices
- Adopt rules for IT security
- Developing a statewide IT security strategic plan, updated annually
- Developing a framework for use by state agencies for IT security responsibilities such as conducting IT security risk assessments and reporting IT security incidents
- Provide IT security training for state agency information security managers
- Annually review state agency IT security plans

Florida currently does not define or specifically address cybersecurity in statute, instead defining IT security. The state's current IT security structure and approach is decentralized and fragmented among individual state agencies – AST, the Florida Department of Law Enforcement (FDLE), and the Division of Emergency Management (DEM). Some entities involved in IT security are established in statute with defined responsibilities, such as the FDLE Cybercrime Office in s. 943.0415, F.S., and state agencies, but others are not, such as the FDLE Fusion Center. Current statutes require the development and implementation of several types of plans to include IT security plans, continuity of business plans and emergency management plans.

Effect of Changes

The bill creates the Florida Cybersecurity Task Force administratively supported by the FDLE to review and provide recommendations for the improvement of the state's cybersecurity infrastructure, governance, and operations. The task force consists of the following members:

- A representative of the computer crime center of the Florida Department of Law Enforcement appointed by the executive director of the department.
- A representative of the fusion center of the Florida Department of Law Enforcement appointed by the executive director of the department.
- The chief information security officer of the Office of Technology and Data Solutions.
- A representative of the Division of Telecommunications of the Department of Management Services appointed by the secretary of the department.
- A representative of the Division of Emergency Management in the Executive Office of the Governor appointed by the director of the division.
- A representative of the Office of the Chief Inspector General in the Executive Office of the Governor appointed by the Chief Inspector General.

The task force is required to submit a final report of its findings and recommendations to the Executive Office of the Governor, the President of the Senate, and the Speaker of the House of Representatives by November 1, 2018.

II. FISCAL ANALYSIS & ECONOMIC IMPACT STATEMENT

A. FISCAL IMPACT ON STATE GOVERNMENT:

1. Revenues: See Fiscal Comments

2. Expenditures: See Fiscal Comments

B. FISCAL IMPACT ON LOCAL GOVERNMENTS:

1. Revenues: None.

2. Expenditures: None.

C. DIRECT ECONOMIC IMPACT ON PRIVATE SECTOR:

The bill requires the State Data Center and state agency customer entities to utilize cloud computing services when beneficial use of these services is validated through cost benefit analyses, which should reduce State Data Center costs in subsequent years.

D. FISCAL COMMENTS:

- The bill conforms to the conference report for Senate Bill 2500 GAA.
  - The positions removed from statute have no funding in the budget except for the chief operations officer, which will be reclassified as the state data center director.
  - The GAA appropriates 50,000 in additional salary rate for the state CIO due to the increased qualifications (does not apply to an interim state CIO).
- The bill appropriates $100,000 in nonrecurring general revenue funds to the Florida Department of Law Enforcement for purposes of administrative support for the Florida Cybersecurity Task Force.