HOUSE OF REPRESENTATIVES STAFF ANALYSIS

BILL #: HB 1171 Division of State Technology
SPONSOR(S): Toledo; Duran and others
TIED BILLS: **IDEN./SIM. BILLS:** SB 800

REFERENCE	ACTION	ANALYST	STAFF DIRECTOR or BUDGET/POLICY CHIEF
1) Oversight, Transparency & Public Management Subcommittee	11 Y, 0 N	Toliver	Smith
2) Appropriations Committee			
3) State Affairs Committee			

SUMMARY ANALYSIS

The Department of Management Services (DMS) oversees IT governance and security for the executive branch of state government. The Division of State Technology (DST), a subdivision of DMS subject to its control and supervision, implements DMS's duties and policies in this area. The head of DST is appointed by the Secretary of Management Services and serves as the state chief information officer. The duties and responsibilities of DMS and DST relating to IT management include:

- Developing IT policy for the management of the state's IT resources;
- Establishing IT architecture standards;
- Establishing project management and oversight standards;
- Performing project oversight of all state agency IT projects that have a total cost of $10 million or more, as well as cabinet agency IT projects that have a total cost of $25 million or more;
- Recommending potential methods for standardizing data across state agencies which will promote interoperability and reduce the collection of duplicative data;
- Recommending open data technical standards and terminologies for use by state agencies;
- Establishing best practices for the procurement of IT products and cloud-computing services in order to reduce costs, increase the quality of data center services, or improve government services;
- Establishing a policy for all IT-related state contracts.

The bill creates the Data Innovation Program within DST. The bill provides that the Legislature recognizes that DMS is responsible for ensuring that the state's data is interoperable. The bill requires DST to:

- Identify all data elements within state agencies and publish a data catalog;
- Develop common data definitions across state agencies and publish a data dictionary;
- Inform state agencies of the data types they collect and report publicly or to the Federal government to identify where interagency data-sharing can create staff and technology efficiencies;
- Inventory, by June 30, 2020, all existing interagency data-sharing agreements, identify areas of data-sharing needs, and, thereafter, execute a new interagency agreement.

To promote data interoperability across government agencies, the bill directs DST to develop three pilot programs in conjunction with the Agency for Health Care Administration, the Department of Health, and the Department of Children and Families. The pilot programs must be conducted by December 31, 2020. The programs must demonstrate interoperability across diverse data types, enable information generation across state agencies with different missions, and be able to scale to provide at volumes to support all types of initiatives. The pilot programs must use solutions that preserve existing investments in technology among agencies while achieving interoperability on a broader scale and enabling future technical paradigms.

The bill may have a negative fiscal impact on state government expenditures.

FULL ANALYSIS

I. SUBSTANTIVE ANALYSIS

A. EFFECT OF PROPOSED CHANGES:

Background

Department of Management Services

IT Management

The Department of Management Services (DMS)[1] oversees information technology (IT)[2] governance and security for the executive branch of state government. The Division of State Technology (DST), a subdivision of DMS subject to its control and supervision, implements DMS's duties and policies in this area.[3] The head of DST is appointed by the Secretary of Management Services[4] and serves as the state chief information officer (CIO).[5] The CIO must be a proven effective administrator with at least 10 years of executive level experience in the public or private sector.[6] DST "provides the State with guidance and strategic direction on a variety of transformational technologies, such as cybersecurity and data analytics, while also providing the following critical services: voice, data, software, and much more."[7] The duties and responsibilities of DMS and DST include:

- Developing IT policy for the management of the state's IT resources;
- Establishing IT architecture standards and assisting state agencies[8] in complying with those standards;
- Establishing project management and oversight standards with which state agencies must comply when implementing IT projects. The standards must include:
  - Performance measurements and metrics that reflect the status of an IT project based on a defined and documented project scope, cost, and schedule;
  - Methodologies for calculating acceptable variances in the projected versus actual scope, schedule, or cost of an IT project; and
  - Reporting requirements
- Performing project oversight of all state agency IT projects that have a total cost of $10 million or more, as well as cabinet agency IT projects that have a total cost of $25 million or more, and are funded in the General Appropriations Act or any other law;
- Recommending potential methods for standardizing data across state agencies which will promote interoperability and reduce the collection of duplicative data;
- Recommending open data[9] technical standards and terminologies for use by state agencies;
- Establishing best practices for the procurement of IT products and cloud-computing services in order to reduce costs, increase the quality of data center services, or improve government services; and
- Establishing a policy for all IT-related state contracts, including state term contracts for IT commodities, consultant services, and staff augmentation services.[10]

---

[1] *See* s. 20.22, F.S.

[2] 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. S. 282.0041(14), F.S.

[3] Section 20.22(2)(a), F.S.

[4] The Secretary of Management Services serves as the head of DMS and is appointed by the Governor, subject to confirmation by the Senate. S. 20.22(1), F.S.

[5] Section 20.22(2)(b), F.S.

[6] *Id.*

[7] *State Technology*, FLORIDA DEPARTMENT OF MANAGEMENT SERVICES , https://www.dms.myflorida.com/business_operations/state_technology (last visited January 27, 2020).

[8] *See* s. 282.0041(27), F.S.

[9] The term "open data" means data collected or created by a state agency and structured in a way that enables the data to be fully discoverable and usable by the public. The term does not include data that are restricted from public distribution based on federal or state privacy, confidentiality, and security laws and regulations or data for which a state agency is statutorily authorized to assess a fee for its distribution. S. 282.0041(18), F.S.

State Data Center and the Cloud-First Policy

In 2008, the Legislature created the State Data Center (SDC) system, established two primary data centers,[11] and required that agency data centers be consolidated into the primary data centers by 2019.[12] Data center consolidation was completed in FY 2013-14. In 2014, the two primary data centers were merged in law to create the SDC within then-existing AST.[13] The SDC is established within DMS and DMS is required to provide operational management and oversight of the SDC.[14]

The SDC relies heavily on the use of state-owned equipment installed at the SDC facility located in the state's Capital Circle Office Center in Tallahassee for the provision of data center services. The SDC is led by the director of the SDC.[15] The SDC is required to do the following:

- Offer, develop, and support the services and applications defined in service-level agreements executed with its customer entities;[16]
- Maintain performance of the state data center by ensuring proper data backup, data backup recovery, disaster recovery, and appropriate security, power, cooling, fire suppression, and capacity;
- Develop and implement business continuity and disaster recovery plans, and annually conduct a live exercise of each plan;
- Enter into a service-level agreement with each customer entity to provide the required type and level of service or services;
- Assume administrative access rights to resources and equipment, including servers, network components, and other devices, consolidated into the SDC;
- Show preference, in its procurement process, for cloud-computing solutions that minimize or do not require the purchasing, financing, or leasing of SDC infrastructure, and that meet the needs of customer agencies, reduce costs, and that meet or exceed the applicable state and federal laws, regulations, and standards for IT security; and
- Assist customer entities in transitioning from state data center services to third-party cloud-computing services procured by a customer entity.

A state agency is prohibited, unless exempted[17] elsewhere in law, from:

- Creating a new agency computing facility or data center;
- Expanding the capability to support additional computer equipment in an existing agency computing facility or data center; or
- Terminating services with the SDC without giving written notice of intent to terminate 180 days before termination.[18]

Cloud computing is "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."[19] In 2019, the Legislature mandated that each agency adopt a cloud-first policy that first considers cloud computing solutions in its technology sourcing strategy for technology

---

[10] Section 282.0051, F.S.
[11] The Northwood Shared Resource Center and the Southwood Shared Resource Center. Ss. 282.204-282.205, F.S. (2008).
[12] Chapter 2008-116, L.O.F.
[13] Chapter 2014-221, L.O.F.
[14] *See* s. 282.201, F.S.
[15] Section 282.201, F.S.
[16] A "customer entity" means an entity that obtains services from DMS. Section 282.0041(7), F.S.
[17] The following entities are exempt from the use of the SDC: the Department of Law Enforcement, the Department of the Lottery's Gaming Systems Design and Development in the Office of Policy and Budget, regional traffic management centers, the Office of Toll Operations of the Department of Transportation, the State Board of Administration, state attorneys, public defenders, criminal conflict and civil regional counsel, capital collateral regional counsel, and the Florida Housing Finance Corporation. Section 282.201(2), F.S.
[18] Section 282.201(3), F.S.
[19] *Special Publication 800-145*, National Institute of Standards and Technology, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf (last visited January 27, 2020). The term "cloud computing" has the same meaning as provided in Special Publication 800-145 issued by the National Institute of Standards and Technology (NIST). Section 282.0041(5), F.S.

initiatives or upgrades whenever possible or feasible.[20] Each agency must, just like the SDC, show a preference for cloud-computing solutions in its procurement process and adopt formal procedures for the evaluation of cloud-computing options for existing applications, technology initiatives, or upgrades.[21]

IT Security

The IT Security Act[22] establishes requirements for the security of state data and IT resources.[23] DMS must designate a state chief information security officer (CISO) to oversee state IT security.[24] The CISO must have expertise in security and risk management for communications and IT resources.[25] DMS is tasked with the following duties regarding IT security:

- Establishing standards and processes consistent with generally accepted best practices for IT security, including cybersecurity.
- Adopting rules that safeguard an agency's data, information, and IT resources to ensure availability, confidentiality, and integrity and to mitigate risks.
- Developing, and annually updating, a statewide IT security strategic plan that includes security goals and objectives for the strategic issues of IT security policy, risk management, training, incident management, and disaster recovery planning including:
    - Identifying protection procedures to manage the protection of an agency's information, data, and IT resources;
    - Detecting threats through proactive monitoring of events, continuous security monitoring, and defined detection processes; and
    - Recovering information and data in response to an IT security incident.
- Developing and publishing for use by state agencies an IT security framework.
- Reviewing the strategic and operational IT security plans of executive branch agencies annually.[26]

The IT Security Act requires the heads of state agencies to designate an information security manager to administer the IT security program of the state agency.[27] In part, the heads of state agencies are also required to annually submit to DMS the state agency's strategic and operational IT security plans; conduct, and update every three years, a comprehensive risk assessment to determine the security threats to the data, information, and IT resources of the state agency; develop, and periodically update, written internal policies and procedures; and ensure that periodic internal audits and evaluations of the agency's IT security program for the data, information, and IT resources of the state agency are conducted.[28]

Effect of the Bill

The bill creates the Data Innovation Program (DIP) within DST. The bill provides that the Legislature recognizes that DMS is responsible for ensuring that the state's data is interoperable. The bill provides that the Legislature, by establishing DIP, intends to:

- Ensure that all state agencies collaborate and synthesize data securely through interoperability.
- Create software and IT portfolio rationalization[29] and procurement to achieve interoperability and reduce the number of standalone applications that do not communicate with one another.
- Minimize costs associated with data management areas.

[20] Section 282.206(1), F.S.
[21] Section 282.206(2)-(3), F.S.
[22] Section 282.318, F.S., is cited as the "Information Technology Security Act."
[23] Section 282.318, F.S.
[24] Section 282.318(3), F.S.
[25] *Id.*
[26] Section 282.318(3), F.S.
[27] Section 282.318(4)(a), F.S.
[28] Section 282.318(4), F.S.
[29] The bill defines "IT portfolio rationalization" to mean the streamlining of existing application portfolio to improve efficiency, reduce complexity, and lower the total cost of ownership through processes including software license optimization, application retirement, server optimization, project rationalization, data storage optimization, retirement of aged and low-value applications, elimination of redundancies, standardization of common technology platforms.

- Ensure accurate procedures for regulation and compliance activities.
- Increase transparency within data-related activities,
- Institute better training and educational practices for the management of data assets.
- Increase the value of this state's data while providing standardized data systems, data policies, and data procedures.
- Aid in the resolution of past and current data issues.
- Facilitate improved monitoring and tracking mechanisms for data quality and other data-related activities.
- Increase overall state data standards, thereby translating data into actionable information and workable knowledge of this state's information technology system.
- Enable state agencies to transform their use of technology to offer services in an effective, efficient, and secure manner.
- Improve the health of all persons in this state.

The bill requires DST to identify all data elements within state agencies and develop common data definitions across state agencies; inform state agencies of the data types they collect and report publicly or to the Federal government, to identify where interagency data-sharing can create staff and technology efficiencies. DST must also publish a comprehensive data catalog and a data dictionary. DST must inventory, by June 30, 2020, all existing interagency data-sharing agreements, identify areas of data-sharing needs, and, thereafter, execute a new interagency agreement.

To promote data interoperability across government agencies, the bill directs DST to develop three pilot programs in conjunction with the Agency for Health Care Administration, the Department of Health, and the Department of Children and Families. The pilot programs must be conducted by December 31, 2020. The programs must demonstrate interoperability across diverse data types, enable information generation across state agencies with different missions, and be able to scale to provide at volumes to support all types of initiatives. However, the programs must respect policy differences in data use among the agencies and require robust consent and security functionality, especially related to personal information. To conserve current resources, the bill requires the programs use solutions that preserve existing IT investments while achieving interoperability on a broader scale and enabling future technical paradigms. Lastly, the pilot programs must:

- Enable the use of information in elemental data form, rather than through document-based methods;
- Use technology with the latest standards and standards deployment to facilitate vendor-agnostic interoperability;
- Select solutions with integrated database technology which natively enable analytics at the interagency and intraagency level; and
- Use technology that supports the spectrum of modern software development technologies including application programming interfaces, web services, and representational state transfer.

B. SECTION DIRECTORY:

Section 1 amends s. 282.0041, F.S., relating to definitions applicable to the IT management act.

Section 2 amends s. 282.0051, F.S., relating to the powers, duties, and functions of DMS under the IT management act.

Section 3 creates s. 282.319, F.S., relating to the Data Innovation Program.

Section 4 provides an effective date of upon becoming a law.

II. FISCAL ANALYSIS & ECONOMIC IMPACT STATEMENT

A. FISCAL IMPACT ON STATE GOVERNMENT:

1. Revenues:

   None.

2. Expenditures:

   The bill might have a negative fiscal impact on state government expenditures as it requires the establishment of a new program within DST and the creation and management of three pilot programs. It is unclear whether these functions can be absorbed within DMS's current resources.

B. FISCAL IMPACT ON LOCAL GOVERNMENTS:

1. Revenues:

   None.

2. Expenditures:

   None.

C. DIRECT ECONOMIC IMPACT ON PRIVATE SECTOR:

None.

D. FISCAL COMMENTS:

None.

III. COMMENTS

A. CONSTITUTIONAL ISSUES:

1. Applicability of Municipality/County Mandates Provision:

   Not applicable. This bill does not appear to affect county or municipal governments.

2. Other:

   None.

B. RULE-MAKING AUTHORITY:

The bill gives DMS the power the administer DIP in s. 282.0051, F.S., and DMS has rulemaking authority to adopt rules to administer that section in s. 282.0051(19), F.S. The bills gives DMS sufficient guidance and parameters to allow the department to develop and promulgate rules, if necessary.

C. DRAFTING ISSUES OR OTHER COMMENTS:

None.

IV. AMENDMENTS/ COMMITTEE SUBSTITUTE CHANGES

None.