The Florida Senate

BILL ANALYSIS AND FISCAL IMPACT STATEMENT

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

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

BILL:	SB 576
INTRODUCER:	Senator Harrell
SUBJECT:	Local Government Cyber Security
DATE:	February 10, 2026
REVISED:	

	ANALYST	STAFF DIRECTOR	REFERENCE	ACTION
1.	Harmsen	McVaney	GO	**Pre-meeting**
2.			AEG	
3.			AP	

I. Summary:

SB 576 creates the Local Government Cybersecurity Protection Program, which will be administered by the Florida Digital Service (FLDS), within the Department of Management Services (DMS), to provide local governments and law enforcement access to programs and software to protect against cybersecurity threats and ransomware incidents. The FLDS must secure federal grants to further the program.

Local governments are required to participate in and apply for the program; fiscally constrained counties will be given priority.

The bill grants the DMS rulemaking authority to adopt an application form for the grant program.

The impact on local government revenues and expenditures is indeterminate. Local government may experience cost savings if it receives programs and software that would otherwise be funded with local revenues, but it may be required to expend funds to accommodate the programs and software if that chosen by the FLDS does not comport with its current information technology strategy.

The bill takes effect July 1, 2026.

II. Present Situation:

The Department of Management Services (DMS) oversees information technology (IT)[1] governance and security for the executive branch in Florida.[2] The Florida Digital Service (FLDS) is housed within the DMS and was established in 2020 to replace the Division of State Technology.[3] The FLDS works under the DMS to implement policies for information technology and cybersecurity for state agencies.[4]

The head of the FLDS is appointed by the Secretary of Management Services[5] and serves as the state chief information officer (CIO).[6] 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.[7] 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.[8]

The DMS, through the FLDS, 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.[9]

State Cybersecurity Act

The State Cybersecurity Act[10] (the Cybersecurity Act) requires the DMS, acting through the FLDS, to establish standards and processes for assessing state agencies' cybersecurity risks and determine appropriate security measures. For purposes of the State Cybersecurity Act, a "state agency" is any official, officer, commission, board, authority, council, committee, or department

[1] 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(20), F.S.
[2] *See* s. 20.22, F.S.
[3] Chapter 2020-161, L.O.F.
[4] *See* s. 20.22(2)(b), F.S.
[5] 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.
[6] Section 282.0051(2)(a), F.S.
[7] *Id.*
[8] Section 282.0051 (1), F.S.
[9] *Id*.
[10] Section 282.318(1), F.S.

of the executive branch and specifically includes the Department of Legal Affairs, the Department of Agriculture and Consumer Services, and the Department of Financial Services, but excludes university boards of trustees or state universities.[11]

Additionally, under the Cybersecurity Act, the DMS must:[12]

- Adopt rules to mitigate risk and to safeguard state agency digital assets, data, information, and IT resources to ensure its confidentiality and integrity;
- Designate a chief information security officer (CISO);
- Develop an annual cybersecurity strategic plan that includes the identification and mitigation of risk, proactive protection against threats, and threat reporting and response and recovery protocols for a cyber incident;
- Publish an IT security framework for use by state agencies;
- Annually review state agencies' strategic and operational cybersecurity plans; and
- Operate a Cybersecurity Operations Center (CSOC), which serves as "a clearinghouse for threat information" and coordinates with the Department of Law Enforcement to support state agencies with their response to a confirmed or suspected cybersecurity incident.

Each state agency is also vested with responsibilities under the Cybersecurity Act, which include:[13]

- Creating a cybersecurity response team that convenes upon notice of a cybersecurity incident and reports on all confirmed or suspected incidents;
- Submitting an annual report on the agency's strategic and operational cybersecurity plans;
- Performing a triennial comprehensive risk assessment to determine security threats to the agency;
- Developing internal procedures, including procedures for reporting cybersecurity incidents and breaches to the Cybercrime Office and the FLDS;
- Receiving recommendations from the DMS regarding identified risks to agency data, information, and IT resources, and implementation of safeguards and risk assessment remediation plans to resolve the risk;
- Ensuring the performance of periodic internal audits and evaluations of the agency's cybersecurity program for the data, information, and IT resources of the agency; and
- Submitting an after-action report, including a summary of "insights gained as a result of the incident" to the FLDS within one week after the agency's resolution or remediation of a cybersecurity incident or ransomware incident.

Local Government Cybersecurity Act

The Local Government Cybersecurity Act (Local Act),[14] which applies to any county or municipality, requires each local government to have adopted by January 1, 2025, cybersecurity standards, consistent with generally accepted best practices, that safeguard its data, IT, and IT resources to ensure availability, confidentiality, and integrity. The Local Act additionally requires a local government to notify the Cybersecurity Operations Center within the Florida

[11] Sections 282.0041(34) and 282.318(2), F.S.
[12] Section 282.318(3), F.S.
[13] Section 282.318(4), F.S.
[14] Section 282.3185, F.S.

Department of Law Enforcement and the sheriff who has jurisdiction over the local government of any cybersecurity or ransomware incident.

The Local Act also requires the FLDS to develop basic and advanced cybersecurity training for local government employees, who must complete the training within 30 days of beginning their employment and annually thereafter. The FLDS may collaborate with the Cybercrime Office of the Department of Law Enforcement, a private sector entity, or an institution of the State University System to develop this training.[15]

Florida Local Government Cybersecurity Grant Program

The Florida Local Government Cybersecurity Grant Program (Grant Program) is currently administered by the FLDS. The Grant Program has been authorized in proviso language beginning with the Fiscal Year (FY) 2023-2024 General Appropriations Act (GAA).[16] Proviso language in the FY 2025-2026 GAA requires the DMS, through the FLDS, to administer a competitive grant program that provides nonrecurring technical assistance to local governments for the development and enhancement of cybersecurity risk management programs. The FLDS is required to include language in the local government agreements that release the state from all liability related to cybersecurity incidents impacting the local government recipient.[17] For FY 2025-26, the Grant Program prioritized fiscally constrained rural areas of opportunity.[18]

The grant itself does not define what constitutes a fiscally constrained county. However, s. 218.67(1), F.S., defines a fiscally constrained county as one that:

- Has been designated by the Governor pursuant to s. 288.0656, F.S.;
- Has been adversely affected by an extraordinary economic event, severe or chronic distress, or a natural disaster that presents a unique economic development opportunity; and
- That meets specified population limits.[19]

Alternatively, a county may be classified as a rural area of opportunity if the value of a mill of ad valorem taxes will raise no more than $5 million in revenue for the county, based on the taxable value used in the determination of funding allocations from the Florida Education Finance Program under s. 1011.62(4)(a)1.a, F.S.

In Fiscal Year 2025-2026, there are 29 fiscally constrained counties.[20]

---

[15] Section 282.3185(3), F.S.
[16] Ch. 2023-239, L.O.F., proviso language for Specific Appropriation 3013A.
[17] Ch. 2025-198, L.O.F., proviso language for Specific Appropriation 2708.
[18] *See* FLDS, *Florida Local Government Cybersecurity Grant Program*, https://cybergrants.fl.gov/ (last visited Feb. 1, 2026).
[19] A rural area of opportunity is a rural community, which is defined in s. 288.0656(2)(e), F.S., as:
1. A county with a population of 75,000 or fewer.
2. A county with a population of 125,000 or fewer which is contiguous to a county with a population of 75,000 or fewer.
3. A municipality within a county described in subparagraph 1. or subparagraph 2.
4. An unincorporated federal enterprise community or an incorporated rural city with a population of 25,000 or fewer and an employment base focused on traditional agricultural or resource-based industries, located in a county not defined as rural, which has at least three or more of the economic distress factors identified in paragraph (c) and verified by the department.

[20] Florida Department of Revenue, *Fiscally Constrained Counties*, https://floridarevenue.com/property/Documents/fcc_map.pdf (last visited Feb. 5, 2026).

The FLDS has chosen to procure cybersecurity solutions[21] directly on behalf of awarded applicants,[22] rather than issue direct funding to local governments through the grant awards. The grants are designed to support the delivery of new or expanded cybersecurity capabilities, and cannot subsidize payments for existing tools, services, or contracts held by a local government. As a condition of award, local governments must agree to grant FLDS permission to see telemetry[23] and solutions[24] data generated by the software awarded to the local government for FLDS to assist with responding to cybersecurity incidents.[25]

The DMS has been appropriated a total of $55 million through FY 2025-2026 for FLDS to administer the Grant Program and has disbursed $35,235,536.88 as of January 29, 2026.[26] From these funds, 278 local governments have received access to cybersecurity solutions.[27]

Federal "State and Local Government Cybersecurity Grant Program"

The State and Local Government Cybersecurity Grant Program (SLCGP) is administered by Department of Homeland Security through the Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Emergency Management Agency (FEMA) at the federal level. The SLCGP made $91.7 million in FY 2025-2026 available to state and local governments "for a range of cybersecurity improvements, including planning and exercises, hiring experts in the community, and improving services for their citizens."[28]

Funding from the SLCGP helps eligible entities address cybersecurity risks and threats to information systems owned or operated by—or on behalf of—SLCGP governments.[29] State

---

[21] *See*, FLDS, *Florida Local Government Cybersecurity Grant Program—Cybersecurity Capabilities*, https://cybergrants.fl.gov/capabilities.html (last visited January 31, 2026).

[22] *See* FLDS, *Florida Local Government Cybersecurity Grant Program—About the FY 2025-26 Program*, https://cybergrants.fl.gov/ (last visited January 31, 2026) ("Rather than issuing direct funding, the Florida Digital Service will procure cybersecurity solutions directly on behalf of awarded applicants. No payments will be made to grant recipients.")

[23] FLDS, *Local Government Cybersecurity Grant Program Grant Agreement—Exhibit A, Cybersecurity Incident Response Rider*, https://cybergrants.fl.gov/download/Year_3_Local_Grant_Agreement_FY2025-26_Draft.pdf (last visited Jan. 31, 2026). ("Telemetry data" means data generated by Grantee through automated communication processes from multiple data sources and processed by Software Entitlements.)

[24] *Id*. at 33. "Solution data" is defined as data, reports, or other information generated by Software Entitlements. This may be derived from, but does not include Telemetry Data.

[25] *Id*.

[26] *See* Dep't. of Management Services, Technology Program, *2024-25 Disbursements by Summary Object: Special Categories ~ Grants and Aids – Cybersecurity Grants*, TRANSPARENCY FLORIDA, https://www.transparencyflorida.gov/Disbursements/DisbBySummObj.aspx?FY=25&BE=72900700&AC=100856&Fund=1000&FundType=&LI=*****&OB=Y&SC=F (last visited Feb. 3, 2025); Dep't of Management Services, Technology Program, *2025-26 Disbursements by Summary Object: Special Categories ~ Grants and Aids – Cybersecurity Grants*, TRANSPARENCY FLORIDA, available at https://www.transparencyflorida.gov/Disbursements/DisbBySummObj.aspx?FY=25&BE=72900700&AC=100856&Fund=1000&FundType=&LI=*****&OB=Y&SC=F (last visited Feb. 3, 2026).

[27] *See* FLDS, *FY 2024-2025 Florida Local Government Cybersecurity Grant Program Report Round 1 and FY 2024-2025 Florida Local Government Cybersecurity Grant Program Report Round 2* (on file with the Information Technology Budget and Policy Subcommittee).

[28] Cybersecurity and Infrastructure Security Agency (CISA), *DHS Launches Over $100 Million in Funding to Strengthen Communities' Cyber Defenses* (Aug. 1, 2025), https://www.cisa.gov/news-events/news/dhs-launches-over-100-million-funding-strengthen-communities-cyber-defenses (last visited Feb. 1, 2026).

[29] CISA, *State and Local Cybersecurity Grant Program,* https://www.cisa.gov/cybergrants/slcgp (last visited Feb. 1, 2026).

Administrative Agencies may apply to receive SLCGP funds from the federal government and, if awarded, must distribute at least 80 percent of the funding to local governments in accordance with state law, procedures, and federal legislative requirements.[30] At least 25 percent of the distributed funds must go to rural areas of the state.[31] However, the state entity must match the federal funds with a 40 percent match.[32] In Fiscal Year 2023-2024, Florida received $11,997,340 from the SLCGP; in Fiscal Year 2024-2025, it received $8,704,903.[33]

III. Effect of Proposed Changes:

The bill creates the Local Government Cybersecurity Protection Program (program), which will be administered by the Florida Digital Service (FLDS), within the Department of Management Services (DMS), to give local governments and law enforcement access to programs and software to protect against cybersecurity threats and ransomware incidents.

The FLDS must secure and administer federal grants to further the program by awarding information technology (IT) commodities and services directly to local governments. Florida's 29 fiscally constrained counties[34] will be given priority in the program. The bill defines a fiscally constrained county as it is defined in s. 218.67(1), F.S.,–a county entirely within a rural area of opportunity (as designated by the Governor pursuant to s. 288.0656, F.S.), or each county for which the value of a mill of ad valorem taxes will raise no more than $5 million in revenue.

The program requires each local government to participate in the program and to apply to the FLDS for use of cybersecurity programs and software on an application form prescribed by the DMS.

The bill grants rulemaking authority to the DMS to implement the bill and specifically directs the DMS to adopt an application form for local governments to apply for the program.

The bill takes effect July 1, 2026.

IV. Constitutional Issues:

A. Municipality/County Mandates Restrictions:

Not applicable. The bill does not require counties or municipalities to take an action requiring the expenditure of funds, reduce the authority that counties or municipalities

[30] CISA, *State and Local Cybersecurity Grant Program Fact Sheet Pass-through Requirements* (Aug. 12, 2025), https://www.cisa.gov/resources-tools/resources/state-and-local-cybersecurity-grant-program-fact-sheet (last visited Feb. 1, 2026).
[31] CISA, *State and Local Cybersecurity Grant Program Fact Sheet, Cost Share Requirements* (Aug. 12, 2025), https://www.cisa.gov/resources-tools/resources/state-and-local-cybersecurity-grant-program-fact-sheet (last visited Feb. 1, 2026).
[32] *Id*.
[33] Federal Emergency Management Agency, *State and Local Cybersecurity Grant Program Funding Allocations*, https://www.fema.gov/grants/preparedness/state-local-cybersecurity-grant-program/funding_allocations (last visited Feb. 1, 2026).
[34]

have to raise revenue in the aggregate, nor reduce the percentage of state tax shared with counties or municipalities.

B. Public Records/Open Meetings Issues:

None.

C. Trust Funds Restrictions:

None.

D. State Tax or Fee Increases:

None.

E. Other Constitutional Issues:

None identified.

V. Fiscal Impact Statement:

A. Tax/Fee Issues:

None.

B. Private Sector Impact:

If the FLDS purchases software or other IT commodities for the grant program from a vendor, then the vendor may benefit from funds that would not have otherwise been spent.

C. Government Sector Impact:

Local governments may see a decrease in their costs associated with cybersecurity threat and ransomware incident IT resources because of the FLDS' purchase of said commodities on their behalf. However, the local government may see associated costs with retrofitting its IT, purchasing additional licenses, or staff training to accommodate the resources chosen for it by the FLDS.

The FLDS may see an increase in cost for the administration of the grant program and review of applications by local governments. This can likely be absorbed into existing resources.

VI. Technical Deficiencies:

Lines 27-28 refer to "local governments and law enforcement." Section 282.3185, F.S., defines a "local government" as any county or municipality (which would include law enforcement run by those entities), but this definition does not extend to s. 282.31855, F.S., as created by this bill. The Legislature could either create the grant program under s. 282.3185, F.S., to adopt the

definition of "local government;" or, in the alternative, create a definition of "local government and law enforcement" in s. 282.31855, F.S.

The bill requires all local governments to both participate in and apply to the grant program, but the term "participate" is not defined. Similarly, it is unclear how the grant program will be administered and if there will be enough commodities to give to all counties. It is, therefore, unknown whether there will be sufficient funds to allow each local government to participate (whether or not it wishes to).

It is unclear at what point in time a local government's participation must occur because there is no deadline for their application or participation. If the FLDS administers the grant program created by this bill in the same manner as its Florida Local Government Cybersecurity Grant Program, then the application window would likely operate from July 11-August 31, 2026; with grant award notices and software access beginning in the next calendar year.

The DMS may not be able to adopt an application form by rule prior to the July 11 application opening date, if the FLDS continues to operate its grant program on the same cycle as the past two years. An earlier effective date may facilitate more timely adoption of such a form.

VII. Related Issues:

In some instances, the cybersecurity commodities provided by the FLDS may not prove helpful to the local governments, either because they provide less security than programs and software the local governments currently use, or because of compatibility with other software and programs already procured by the local government. However, the bill will compel such local governments to use the FLDS commodity despite these concerns.

VIII. Statutes Affected:

This bill creates section 282.31855 of the Florida Statutes.

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.