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 Appropriations Committee

BILL:	CS/SB 576
INTRODUCER:	Governmental Oversight and Accountability Committee and Senator Harrell
SUBJECT:	Local Government Cybersecurity
DATE:	February 17, 2026 REVISED:

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

Please see Section IX. for Additional Information:

COMMITTEE SUBSTITUTE - Substantial Changes

I. Summary:

CS/SB 576 creates the Local Government Cybersecurity Protection Program, which will be administered by the Florida Digital Service (FLDS), to provide information technology (IT) commodities and services to local government participants to develop and enhance their cybersecurity risk management programs consistent with s. 282.3185, F.S., and to assist local governments with mitigation and defense against cybersecurity threats, including ransomware incidents. The FLDS may use federal grants to further the program.

The program will be administered based on objective eligibility and evaluation criteria and will prioritize fiscally constrained counties.

The bill requires the FLDS to enter into data-sharing agreements with local governments as necessary to facilitate the collection, analysis, and exchange of security-related information to support the detection, prevention, and response to cybersecurity incidents.

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.

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 2025-2026, the Grant Program prioritized local governments that are fiscally constrained, within 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]

---

[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).

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 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]

Public Records Law

The State Constitution provides that the public has the right to inspect or copy records made or received in connection with official governmental business.[34] This applies to the official business of any public body, officer, or employee of the state, including all three branches of state government, local governmental entities, and any person acting on behalf of the government.[35]

Additional requirements and exemptions that relate to public records are found in various statutes and rules, depending on the branch of government involved.[36] For instance, Legislative records are public pursuant to s. 11.0431, F.S. Public records exemptions for the Legislature are codified primarily in s. 11.0431(2)-(3), F.S., and adopted in the rules of each house of the legislature. Florida Rule of Judicial Administration 2.420 governs public access to judicial branch records.[37] Lastly, ch. 119, F.S., the Public Records Act, provides requirements for public records held by executive agencies and constitutes the main body of public records laws.

The Public Records Act provides that all state, county, and municipal records are open for personal inspection and copying by any person. Each agency has a duty to provide access to public records.[38]

Section 119.011(12), F.S., defines "public records" to include:

> [a]ll documents, papers, letters, maps, books, tapes, photographs, films, sound recordings, data processing software, or other material, regardless

[29] CISA, *State and Local Cybersecurity Grant Program,* https://www.cisa.gov/cybergrants/slcgp (last visited Feb. 1, 2026).
[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] FLA. CONST. art. I, s. 24(a).
[35] *Id*. *See also*, *Sarasota Citizens for Responsible Gov't v. City of Sarasota*, 48 So. 3d 755, 762-763 (Fla. 2010).
[36] Chapter 119, F.S., does not apply to legislative or judicial records. *See*, *Locke v. Hawkes*, 595 So. 2d 32, 34 (Fla. 1992); *see also Times Pub. Co. v. Ake*, 660 So. 2d 255 (Fla. 1995).
[37] *State v. Wooten*, 260 So. 3d 1060 (Fla. 4th DCA 2018).
[38] Section 119.01(1), F.S.

> of the physical form, characteristics, or means of transmission, made or received pursuant to law or ordinance or in connection with the transaction of official business by any agency.

The Florida Supreme Court has interpreted this definition to encompass all materials made or received by an agency in connection with official business which are used to "perpetuate, communicate, or formalize knowledge of some type."[39]

The Florida Statutes specify conditions under which public access to governmental records must be provided. The Public Records Act guarantees every person's right to inspect and copy any state or local government public record at any reasonable time, under reasonable conditions, and under supervision by the custodian of the public record.[40] A violation of the Public Records Act may result in civil or criminal liability.[41]

Only the Legislature may create an exemption to public records requirements.[42] An exemption must be created by general law and must specifically state the public necessity justifying the exemption.[43] Further, the exemption must be no broader than necessary to accomplish the stated purpose of the law. A bill enacting an exemption may not contain other substantive provisions[44] and must pass by a two-thirds vote of the members present and voting in each house of the Legislature.[45]

When creating a public records exemption, the Legislature may provide that a record is "exempt" or "confidential and exempt." There is a difference between records the Legislature has determined to be exempt from the Public Records Act and those which the Legislature has determined to be exempt from the Public Records Act *and confidential*.[46] Records designated as "confidential and exempt" are not subject to inspection by the public and may only be released under the circumstances defined by statute.[47] Records designated as "exempt" may be released at the discretion of the records custodian under certain circumstances.[48]

General exemptions from the public records requirements are typically contained in the Public Records Act.[49] Specific exemptions are often placed in the substantive statutes which relate to a particular agency or program.[50]

---

[39] *Shevin v. Byron, Harless, Schaffer, Reid and Assoc. Inc*., 379 So. 2d 633, 640 (Fla. 1980).
[40] Section 119.07(1)(a), F.S.
[41] Section 119.10, F.S. Public records laws are found throughout the Florida Statutes, as are the penalties for violating those laws.
[42] FLA. CONST. art. I, s. 24(c).
[43] *Id.*
[44] The bill may, however, contain multiple exemptions that relate to one subject.
[45] FLA. CONST. art. I, s. 24(c)
[46] *WFTV, Inc. v. The Sch. Bd. of Seminole County*, 874 So. 2d 48, 53 (Fla. 5th DCA 2004).
[47] *Id.*
[48] *Williams v. City of Minneola*, 575 So. 2d 683 (Fla. 5th DCA 1991).
[49] *See, e.g.*, s.119.071(1)(a), F.S., exempting from public disclosure examination questions and answer sheets of exams administered by a governmental agency for the purpose of licensure.
[50] *See, e.g.*, s. 213.053(2), F.S., exempting from public disclosure information received by the DOR, including investigative reports and information.

Agency Cybersecurity Public Records Exemption, Section 119.0725, F.S.

Section 119.0725(2), F.S., makes confidential and exempt from the public inspection and copying requirements the following cybersecurity-related information:[51]

- Coverage limits and deductible or self-insurance amounts of insurance or other risk mitigation coverages acquired for the protection of information technology (IT)[52] systems, operational technology[53] systems, or an agency's data;
- Information relating to "critical infrastructure", defined as existing and proposed IT and operational technology systems and assets (physical or virtual), the incapacity or destruction of which would negatively affect security, economic security, public health, or public safety;
- Cybersecurity[54] incident information (whether the incident was actual or merely threatened) reported by state agencies or local governments pursuant to ss. 282.318 and 282.3185, F.S.; and
- Network schematics; hardware and software configurations; encryption information; or information that identifies detection, investigation, or response practices for suspected or confirmed cybersecurity incidents, including suspected or confirmed breaches, if the disclosure of such information would facilitate unauthorized access to or unauthorized modification, disclosure, or destruction of:
  - Data[55] or information (physical or virtual); or
  - IT resources, which include an agency's existing or proposed IT systems.

An agency *must* make this information available to a law enforcement agency, the Auditor General, the Cybercrime Office of the FDLE, the Florida Digital Service (FLDS), and—for agencies under the jurisdiction of the Governor—the Chief Inspector General. An agency *may* disclose the confidential and exempt information addressed in s. 119.0725, F.S., "in the furtherance of its official duties and responsibilities or to another agency or governmental entity in the furtherance of its statutory duties and responsibilities."[56]

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). The grant program is intended to provide IT commodities and services to local governments in order to assist eligible local governments with the mitigation of and defense against cybersecurity threats, including ransomware incidents.

---

[51] Section 119.0725(2), F.S. This public records exemption was implemented in 2022, after s. 282.318, F.S., was passed, to better address ransomware incidents.

[52] "Information technology" is defined in s. 119.0725(1)(f), F.S., as "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."

[53] "Operational technology" is the hardware and software that causes or detects a change through the direct monitoring or control of physical devices, systems, processes, or events. Section 119.0725(1)(g), F.S.

[54] Section 119.0725(1)(c), F.S., defines "cybersecurity" as the protection afforded to an automated information system to attain the applicable objectives of preserving the confidentiality, integrity, and availability of data, information, and information technology resources.

[55] "Data" is the subset of structured information in a format that allows such information to be electronically retrieved and transmitted. Section 282.0041(9), F.S.

[56] Section 119.0725(5), F.S.

The FLDS will contract to procure such IT commodities and services on behalf of grant participants.

The FLDS must administer the grant based on objective eligibility and evaluation criteria and give preference to fiscally constrained counties. Florida has 29 fiscally constrained counties[57] as defined in s. 218.67(1), F.S., which includes 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 FLDS must enter into data-sharing agreements with local government grant participants as necessary to facilitate the collection, analysis, and exchange of security-related information to support the detection, prevention, and response to cybersecurity incidents consistent with s. 282.318, F.S.

The FLDS may use federal grants to further the program by awarding information technology (IT) commodities and services directly to local governments.

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 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:

The bill requires local governments that participate in the grant program to enter into data-sharing agreements with the FLDS "as necessary" to facilitate the collection, analysis, and exchange of security-related information to support the detection, prevention, and response to cybersecurity incidents.

This information may be protected by s. 119.0725(2), F.S., which makes exempt the network schematics; hardware and software configurations; encryption information; or information that identifies detection, investigation, or response practices for suspected or confirmed cybersecurity incidents, including suspected or confirmed breaches, if the disclosure of such information would facilitate unauthorized access to or unauthorized modification, disclosure, or destruction of:

- Data[58] or information (physical or virtual); or
- IT resources, which include an agency's existing or proposed IT systems.

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

[58] "Data" is the subset of structured information in a format that allows such information to be electronically retrieved and transmitted. Section 282.0041(9), F.S.

However, if the "security-related information" required to be shared with the FLDS by this bill is not considered information that identifies detection, investigation, or response practices for suspected or confirmed cybersecurity incidents, then a separate public records exemption may be required to protect this information in the hands of FLDS.

C. Trust Funds Restrictions:

None.

D. State Tax or Fee Increases:

None.

E. Other Constitutional Issues:

The bill requires local governments that participate in the grant program to enter into data-sharing agreements with the FLDS "as necessary" to facilitate the collection, analysis, and exchange of security-related information to support the detection, prevention, and response to cybersecurity incidents.

This information may be protected by s. 119.0725(2), F.S., which makes exempt the network schematics; hardware and software configurations; encryption information; or information that identifies detection, investigation, or response practices for suspected or confirmed cybersecurity incidents, including suspected or confirmed breaches, if the disclosure of such information would facilitate unauthorized access to or unauthorized modification, disclosure, or destruction of:

- Data[59] or information (physical or virtual); or
- IT resources, which include an agency's existing or proposed IT systems.

However, if the "security-related information" required to be shared with the FLDS by this bill is not considered information that identifies detection, investigation, or response practices for suspected or confirmed cybersecurity incidents, then a separate public records exemption may be required to protect this information in the hands of FLDS.

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.

[59] "Data" is the subset of structured information in a format that allows such information to be electronically retrieved and transmitted. Section 282.0041(9), F.S.

C. Government Sector Impact:

The FLDS may see an increase in costs 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:

The bill awards grants to "local governments." 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" in s. 282.31855, F.S.

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. It is unclear at what point in the grant process the IT commodities and software that will be made available by the FLDS will be known.

VIII. Statutes Affected:

This bill creates section 282.31855 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 by Governmental Oversight and Accountability on February 11, 2026:

- Removes the requirement that a local government must apply for and participate in the grant program.
- Makes optional, instead of required, that FLDS secure and administer federal grants to further the program.
- Requires the FLDS to enter into data-sharing agreements with local governments that participate in the grant program as necessary to facilitate the collection, analysis, and exchange of security-related information to support cybersecurity threat detection, prevention, and response.
- Requires the FLDS to determine grants based on objective eligibility and evaluation criteria.

B. Amendments:

None.