FLORIDA HOUSE OF REPRESENTATIVES
BILL ANALYSIS

This bill analysis was prepared by nonpartisan committee staff and does not constitute an official statement of legislative intent.

BILL #: CS/HB 1085	**COMPANION BILL:** SB 576 (Harrell)
TITLE: Local Government Cyber Security	**LINKED BILLS:** None
SPONSOR(S): Miller	**RELATED BILLS:** None

Committee References

Information Technology Budget & Policy
15 Y, 0 N, As CS
➤ Intergovernmental Affairs
➤ State Affairs

SUMMARY

Effect of the Bill:
The bill creates the Local Government Cybersecurity Protection Program (the Program), to be administered by the Florida State University (FSU), to assist eligible local governments with developing and enhancing cybersecurity risk management programs to mitigate and defend against cybersecurity threats. The bill authorizes FSU to contract for information technology (IT) commodities and services and provide them to eligible local governments. The bill requires FSU to award grants annually by October 1 and give preference to fiscally constrained counties. FSU must also enter into data-sharing agreements with local governments and the Florida Digital Service (FLDS) necessary to support the detection, prevention, and response to cybersecurity incidents consistent with the State Cybersecurity Act. The bill authorizes FSU to apply for and accept any funds or grants made available by any agency or department of the Federal Government to further the Program.

Fiscal or Economic Impact:
The bill may have a significant negative fiscal impact on state government if additional state funding is requested by FSU to implement the requirements of the bill. It is unknown if there are federal grants available to FSU to implement the Program which would offset the need for state funds. The overall fiscal impact is indeterminate.

JUMP TO SUMMARY ANALYSIS RELEVANT INFORMATION BILL HISTORY

ANALYSIS

EFFECT OF THE BILL:

The bill creates the Local Government Cybersecurity Protection Program (the Program) to be administered by the Florida State University (FSU). The purpose of the Program is to assist eligible local governments with mitigating and defending against cybersecurity threats, which include, but are not limited to, ransomware incidents. The Program's purpose will be accomplished through the award of information technology (IT) commodities and services directly to local governments for use in developing and enhancing an awarded local government's cybersecurity risk management program consistent with the Local Government Cybersecurity Act.[1] (Section 1)

The bill authorizes FSU to contract for IT commodities and services and award them to local governments through the Program based on objective eligibility and evaluation criteria. The bill requires FSU to award grants annually by October 1 and specifies that fiscally constrained counties receive preference in the Program. (Section 1)

The bill requires FSU to enter into data-sharing agreements with local governments and the Florida Digital Service (FLDS). The data-sharing agreements are necessary to facilitate the collection, analysis, and exchange of security-related information to support the detection, prevention, and response to cybersecurity incidents consistent with the State Cybersecurity Act.[2] (Section 1)

[1] S. 282.3185, F.S.
[2] S. 282.318, F.S.

The bill authorizes FSU to apply for and accept any funds or grants to further the Program that are made available to the university by any agency or department of the Federal Government. (Section 1)

The effective date of the bill is July 1, 2026. (Section 2)

FISCAL OR ECONOMIC IMPACT:

STATE GOVERNMENT:

The bill may have a significant negative fiscal impact on state government if additional state funding is requested by FSU to implement the requirements of the bill. It is unknown if there are federal grants available to FSU to implement the Program which would offset the need for state funds. The overall fiscal impact is indeterminate.

RELEVANT INFORMATION

SUBJECT OVERVIEW:

Florida Local Government Cybersecurity Grant Program

The Florida Local Government Cybersecurity Grant Program (FLGCGP) is currently administered by the Florida Digital Service (FLDS) within the Department of Management Services. The FLGCGP has been authorized in proviso language beginning with the Fiscal Year (FY) 2023-2024 General Appropriations Act (GAA).[3] 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 releases the state from all liability related to cybersecurity incidents impacting the local government recipient.[4] For FY 2025-26, the FLGCGP prioritizes fiscally constrained rural areas of opportunity.[5]

The FLDS has chosen, rather than issuing direct funding to local governments through the grant awards, to procure cybersecurity solutions[6] directly on behalf of awarded applicants.[7] 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

[3] Chapter 2023-239, Laws of Florida; proviso language for Specific Appropriation 3013A (last visited January 29, 2026).
[4] Chapter 2025-198, Laws of Florida; proviso language for Specific Appropriation 2708 (last visited January 29, 2026).
[5] *See* Florida Local Government Cybersecurity Grant Program (last visited January 29, 2026).
[6] *See* Florida Local Government Cybersecurity Grant Program. Cybersecurity Capabilities (last visited January 29, 2026).
[7] *See* Florida Local Government Cybersecurity Grant Program (last visited January 29, 2026).

permission to see telemetry[8] and solutions[9] data generated by the software awarded to the local government for FLDS to assist with responding to cybersecurity incidents.[10]

The DMS has been appropriated a total of $55 million through FY 2025-2026 for FLDS to administer the FLGCGP, and has disbursed $35,235,536.88 as of January 29, 2026.[11] From these funds, 278 local governments have received access to cybersecurity solutions awarded through the FLGCGP.[12]

Florida Digital Service

The Florida Digital Service (FLDS), created within the Department of Management Services (DMS), aims to securely modernize state government to achieve value through digital transformation and interoperability and to support the state's cloud-first policy.[13] The Secretary of DMS designates an employee of FLDS as the state chief information security officer (CISO)[14] responsible for the development, operation, and oversight of state cybersecurity.

State Cybersecurity Act

The State Cybersecurity Act (Act)[15] designates DMS, acting through FLDS, as the lead entity responsible for establishing cybersecurity standards and processes for state agencies.[16] These measures must align with best practices, including the National Institute for Standards and Technology (NIST) Cybersecurity Framework (CSF)[17], mitigate risks, safeguard digital assets, and support a security governance framework.[18]

Under the Act, FLDS is responsible for operating a primarily virtual Cybersecurity Operations Center (CSOC), led by the CISO and staffed with FLDS personnel responsible for threat detection and incident response. The CSOC serves as a threat information clearinghouse and coordinates with FDLE to assist state agencies and local governments requesting assistance with incident response.[19]

Further, the Act requires FLDS to annually provide cybersecurity training to all state agency technology professionals and employees with access to highly sensitive information which develops, assesses, and documents competencies by role and skill level. The cybersecurity training curriculum must include training on the identification of each cybersecurity incident severity level.[20] The training curriculum required under the Act serves as the basis for the cybersecurity training curriculum required to be developed by FLDS for local governments.[21]

Current Cybersecurity Practices and Programs at the Florida State University

The Information Technology Services Information Security and Privacy Office (ISPO) is responsible for protecting

---

[8] As defined in Exhibit A, Cybersecurity Incident Response Rider, of the FLGCGP Grant Agreement, "telemetry data" means data generated by Grantee through automated communication processes from multiple data sources and processed by Software Entitlements.
[9] As defined in Exhibit A, Cybersecurity Incident Response Rider, of the FLGCGP Grant Agreement, "solution data" means data, reports, or other information generated by Software Entitlements. This may be derived from, but does not include, Telemetry Data.
[10] *See* Grant Agreement for Local Government Cybersecurity Grant Program (last visited January 29, 2026).
[11] *See* FY 2024-2025 expenditures and FY 2025-2026 expenditures (last visited January 29, 2026).
[12] *See* Florida Digital Service. 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).
[13] S. 282.0051(1), F.S.; and s. 282.206, F.S.
[14] S. 282.318(3)(a), F.S.
[15] S. 282.318, F.S.
[16] S. 282.318(2), F.S.
[17] *See* NIST, *The NIST Cybersecurity Framework (CSF) 2.0* (last visited January 24, 2026).
[18] S. 282.318(3), F.S.
[19] S. 282.318(3)(h), F.S.
[20] S. 282.318(3)(c)9.a., F.S.
[21] S. 282.3185(3)(a)2., F.S.

the FSU community and infrastructure from cyberattacks.[22] As part of its 2026–2029 cybersecurity strategic plan, the ISPO is tasked with reducing institutional cyber risk through a mix of risk-based policy development, software lifecycle guidance, secure network architecture, and workforce education and awareness initiatives.[23] Cybersecurity services currently provided by the ISPO include, but are not limited to, information security and privacy assessments; risk management services; incident management and response; and training.[24] The ISPO provides several enterprise-wide security tools that are required to be adopted and implemented by all university business units.[25]

In accordance with Florida Board of Governors (BOG) regulations,[26] FSU has established cybersecurity standards which include requirements and best practices to preserve the confidentiality, integrity, and availability of the university's information technology assets.[27] The FSU has adopted the NIST CSF[28] as the foundation for a risk-based approach to cybersecurity management. The NIST CSF serves as the standard for policies adopted by the university, such as the Information Technology Application Secure Coding Standard,[29] the Information Technology Enterprise Integration Security Standard,[30] and the Data Security Standard.[31] Additionally, all software and web applications must meet Open Worldwide Application Security Project (OWASP) Secure Coding Requirements[32] or their equivalent.

Local Government Cybersecurity

Current law requires local governments to implement, adopt, and comply with cybersecurity training, standards, and incident notification protocols.[33] The FLDS is responsible for developing cybersecurity training for local government employees. All employees with access to a local government's network must complete basic cybersecurity training within 30 days of employment and annually thereafter. Additionally, technology professionals and employees handling highly sensitive information must complete advanced cybersecurity training on the same schedule.[34]

Local governments must also adopt cybersecurity standards that protect their data, information technology, and information technology resources while ensuring availability, confidentiality, and integrity. These standards must align with generally accepted best practices, including the NIST CSF.[35] Once adopted, local governments must notify FLDS as soon as possible.[36]

In the event of a cybersecurity or ransomware incident, local governments must adhere to specific notification protocols. They are required to notify the CSOC,[37] the Cybercrime Office of FDLE, and the local sheriff. At a minimum, the notification must include a summary of the incident, the date and location of the most recent data

---

[22] *See* Florida State University, Information Technology Services Information Security and Privacy Office (last visited January 24, 2026).
[23] *See* Florida State University, Office of Information Security and Privacy Operations. Cybersecurity Strategic Plan 2026–2029 (last visited January 24, 2026)
[24] *See* Florida State University, Information Security and Privacy Office Charter (last visited January 24, 2026).
[25] *See* Florida State University, Institutional Security (last visited January 24, 2026)
[26] *See* Board of Governors, Regulation 3.0075 – Security of Data Related Information Technology Resources (last visited January 24, 2026).
[27] *See* Florida State University, Cybersecurity Standards and Best Practices (last visited January 24, 2026).
[28] *See* NIST, *The NIST Cybersecurity Framework (CSF) 2.0* (last visited January 24, 2026).
[29] *See* Florida State University, 4-OP-H-25.16 IT Application Secure Coding Standard (last visited January 24, 2026).
[30] *See* Florida State University, 4-OP-H-25.17 IT Enterprise Integration Security Standard (last visited January 24, 2026).
[31] *See* Florida State University, 4-OP-H-25.01 Data Security Standard (last visited January 24, 2026).
[32] *See* OWASP, Application Security Verification Standard 5.0.0 (last visited January 24, 2026).
[33] S. 282.3185, F.S.
[34] S. 282.3185(3), F.S.
[35] *See* NIST, *The NIST Cybersecurity Framework (CSF) 2.0* (last visited January 24, 2026).
[36] S. 282.3185(4), F.S.
[37] The CSOC, led by the state chief information security officer within FLDS, is a primarily virtual facility staffed with detection and incident response personnel that serves as a clearinghouse for cybersecurity threat information and coordinates with law enforcement. *See* s. 282.318(3)(h), F.S.

backup—including whether it was affected or stored in the cloud—the types of data compromised, the estimated financial impact, and, in the case of ransomware, the ransom demand details. Additionally, the local government must indicate whether it is requesting assistance from the CSOC, FDLE, or the sheriff.[38]

Ransomware incidents, as well as cybersecurity incidents classified as severity level 3, 4, or 5, must be reported as soon as possible, but no later than 48 hours after discovery for cybersecurity incidents and 12 hours after discovery for ransomware incidents. The CSOC must then notify the President of the Senate and Speaker of the House of Representatives within 12 hours of receiving the local government's report, providing a high-level description and the likely effects of the incident. Local governments may also report lower-severity cybersecurity incidents at their discretion. The CSOC must also submit a consolidated incident report on a quarterly basis to the President of the Senate, the Speaker of the House of Representatives, and the Florida Cybersecurity Advisory Council (CAC).[39]

Following remediation, an after-action report summarizing the incident, resolution, and lessons learned must be submitted to FLDS within one week. This report must include details such as the incident summary, incident resolutions, and any insights gained as a result of the incident.[40]

BILL HISTORY

COMMITTEE REFERENCE	ACTION	DATE	STAFF DIRECTOR/ POLICY CHIEF	ANALYSIS PREPARED BY
Information Technology Budget & Policy Subcommittee	15 Y, 0 N, As CS	1/28/2026	Davila	Loe
THE CHANGES ADOPTED BY THE COMMITTEE:	• Revised the program from a mandatory model to a voluntary, competitive grant program for local governments. • Revised the program scope from required use of FSU programs and tools to contracted cybersecurity commodities and services awarded based on objective eligibility and evaluation criteria. • Added requirement for FSU to enter into data-sharing agreements with local governments and the Florida Digital Service for security information exchange. • Required FSU to administer grants and award them by October 1 annually.			
Intergovernmental Affairs Subcommittee				
State Affairs Committee				

THIS BILL ANALYSIS HAS BEEN UPDATED TO INCORPORATE ALL OF THE CHANGES DESCRIBED ABOVE.

---

[38] S. 282.3185(5)(b), F.S.

[39] The CAC is an advisory body, housed with the Department of Management Services, tasked with assisting state and local government agencies on addressing cybersecurity threats. The CAC provides guidance on best practices, reviews cybersecurity policies, assesses risks, and makes legislative recommendations. It also collaborates with federal agencies and private-sector experts to enhance cybersecurity measures and reports on ransomware trends. *See* s. 282.319, F.S.

[40] S. 282.3185(6), F.S.