

Florida [Digital Service]

Florida League of Cities Presentation

Building a stronger and more resilient
Florida cyber community

August 2024



The Florida Digital Service

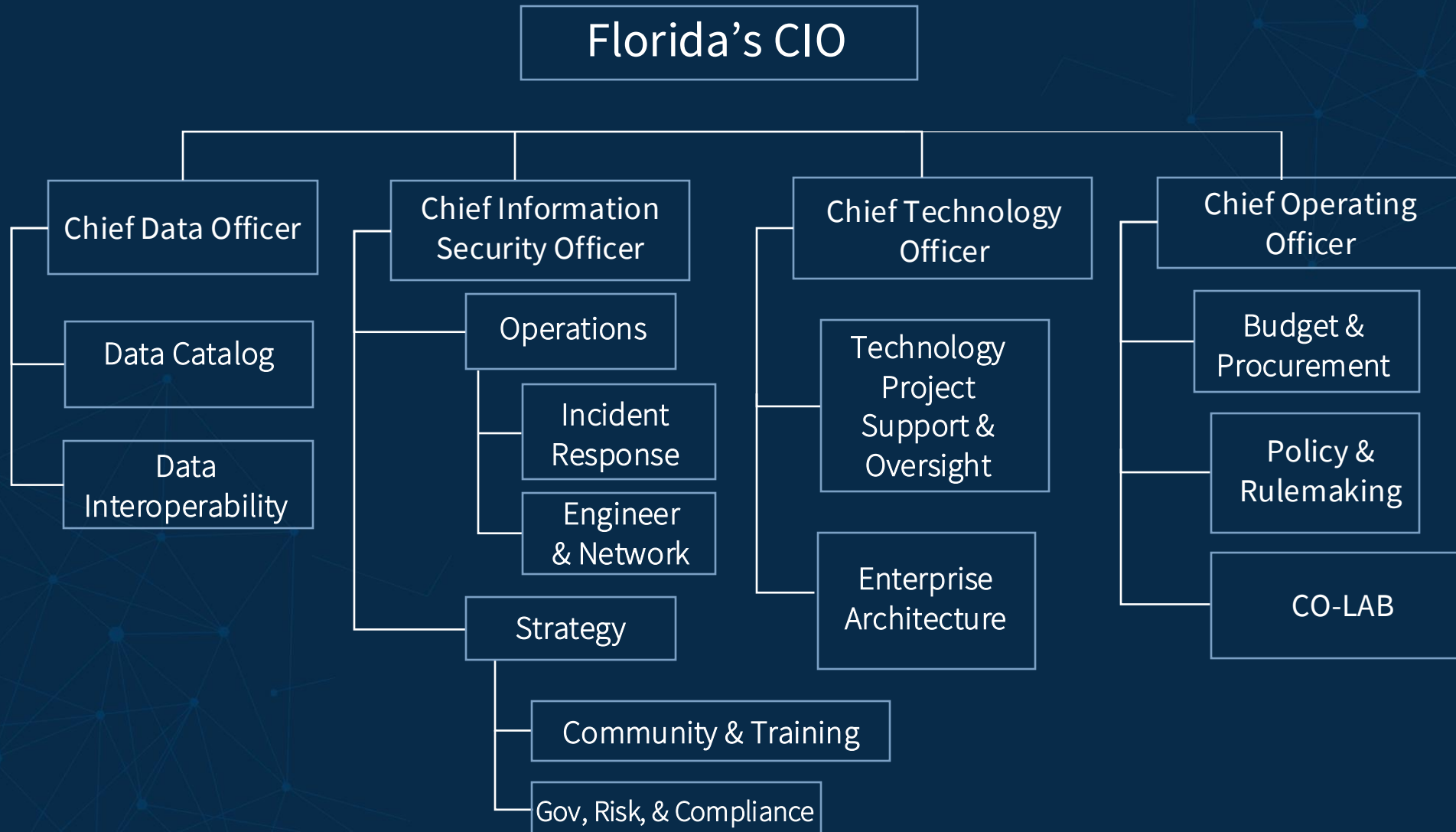
Following Governor Ron DeSantis' call to modernize state government, the Florida Legislature created the Florida Digital Service (FL[DS]) in 2020 to develop and implement the state's enterprise-wide cybersecurity, data interoperability, and cloud-first initiatives to support Florida's government and the constituents who access its critical services.

FL[DS] manages Florida's first State Cybersecurity Operations Center, leads data sharing between state agencies, and leverages the state's purchasing power to deliver taxpayer savings in technology procurement.

FL[DS] is administering the Local Government Cybersecurity Grant Program, a program to provide funding for cybersecurity solutions and services to local Florida governments to improve their cybersecurity posture and resiliency.



The Structure of the Florida Digital Service



What is Cybersecurity?

Cybersecurity is the prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. – *National Institute of Standards and Technology*

Simply Put: Cybersecurity is the practice of protecting computers, networks, and data from damage, theft, and unauthorized access. It ensures that these systems and information are always available, accurate, and private.



Why is Cybersecurity Important?

Protection of Sensitive Information:

- Safeguards personal data.
- Keeps financial information secure.
- Protects government data and public records.

Prevention of Financial Loss:

- Stops cyber attacks that can cost a lot of money in fraud and theft.
- Avoids expenses related to data breaches, including legal fees and fines.

Ensuring Continuity of Services:

- Keeps essential services, like emergency systems and utilities, running smoothly.
- Reduces downtime and service interruptions.

Building Trust with Citizens:

- Citizens rely on their government to keep their information safe.
- Good cybersecurity practices build public confidence.

Compliance with Legal and Regulatory Requirements:

- CJIS, HIPPA, PCI, etc.



F.S. 282.3185 - Local Government Cybersecurity

Responsibilities (1,2,3)

1. Cybersecurity Training
2. Adoption of Cybersecurity Standards
3. Incident Notification and After-Action Reporting



F.S. 282.3185 - Local Government Cybersecurity

282.3185(3) CYBERSECURITY TRAINING

- **Basic Training:** Required for all local government employees with network access. Must be completed within 30 days of employment and annually thereafter.
- **Advanced Training:** Required for local government technology professionals and employees with access to highly sensitive information. Must be completed within 30 days of employment and annually thereafter.



F.S. 282.3185 - Local Government Cybersecurity

282.3185(4) CYBERSECURITY STANDARDS

Cybersecurity Standards: Each local government must adopt standards consistent with best practices, including the NIST Cybersecurity Framework.

Counties:

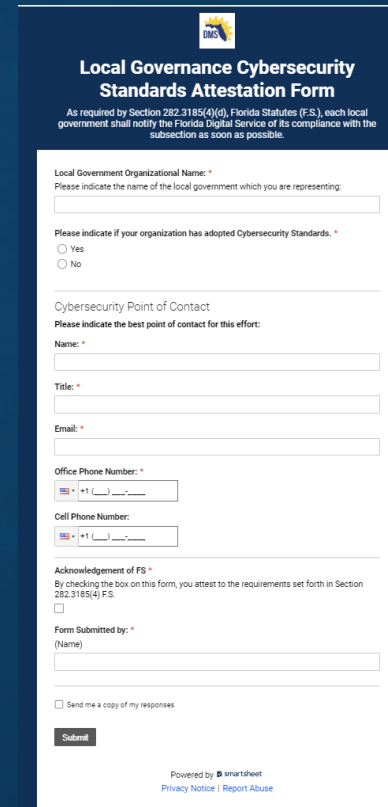
- Population \geq 75,000: Deadline by January 1, 2024
- Population $<$ 75,000: Deadline by January 1, 2025

Municipalities:

- Population \geq 25,000: Deadline by January 1, 2024
- Population $<$ 25,000: Deadline by January 1, 2025

Visit digital.fl.gov/localgovernment-attestation-form

to submit an online attestation, affirming your compliance.



The screenshot shows the 'Local Governance Cybersecurity Standards Attestation Form'. At the top, it features the Florida Digital Service logo and the title 'Local Governance Cybersecurity Standards Attestation Form'. Below the title, a note states: 'As required by Section 282.3185(4)(g), Florida Statutes (F.S.), each local government shall notify the Florida Digital Service of its compliance with the subsection as soon as possible.' The form contains several sections: 'Local Government Organizational Name' with a text input field; 'Please indicate if your organization has adopted Cybersecurity Standards' with radio buttons for 'Yes' and 'No'; 'Cybersecurity Point of Contact' with fields for 'Name', 'Title', and 'Email'; 'Office Phone Number' and 'Cell Phone Number' with phone number input fields; 'Acknowledgement of FS' with a checkbox and explanatory text; and 'Form Submitted by' with a text input field. At the bottom, there is a 'Send me a copy of my responses' checkbox and a 'Submit' button. The footer includes 'Powered by smartswt' and links for 'Privacy Notice' and 'Report Abuse'.



F.S. 282.3185 - Local Government Cybersecurity

282.3185(5 & 6) Incident Notification & After-Action Report

Incident Notification: Local governments must report cybersecurity and ransomware incidents to the Cybersecurity Operations Center (CSOC), the Cybercrime Office of the Florida Department of Law Enforcement (FDLE), and the local Sheriff.

- **Severe Incidents (Level 3, 4, or 5):** Report within 48 hours (cybersecurity)
- **All Ransomware Incidents:** Report within 12 hours.

After-Action Report: Submit a report to the Florida Digital Service within 1 week after incident remediation.



F.S. 282.3185 - Local Government Cybersecurity

282.3185(5 & 6) INCIDENT NOTIFICATION & AFTER-ACTION REPORT

Compliance – CSOC 24/7 Incident Response:

- Online – <https://IR.digital.fl.gov>
- Email – CSOC@digital.fl.gov
- Phone – (850) 412-6074

The screenshot shows the 'CYBERSECURITY INCIDENT REPORTING' web form for state and local governments. The page header includes 'FL [DIGITAL SERVICE]' and navigation links for 'INCIDENT REPORT', 'AFTER ACTION REPORT', and 'INCIDENT SEVERITY'. The main heading is 'CYBERSECURITY INCIDENT REPORTING' with the subtitle 'STATE AND LOCAL GOVERNMENTS'. A paragraph explains that Florida Statute sections 282.318 and 282.3185 require reporting to the CSOC, local Sheriff's office, and FDLE. A 'REPORT AN INCIDENT' section provides contact information for the Florida Digital Service Cybersecurity Operations Center and the Florida Department of Law Enforcement Cybercrime Office. A 'FILL OUT WEB FORM' button is visible, followed by a note about requesting assistance.

FL [DIGITAL SERVICE]

INCIDENT REPORT AFTER ACTION REPORT INCIDENT SEVERITY

CYBERSECURITY INCIDENT REPORTING

STATE AND LOCAL GOVERNMENTS

Per Florida Statute sections 282.318 and 282.3185, state and local governments are required to provide a report to the FL cybersecurity operations center (CSOC), their local Sheriff's office (local governments only) and the Florida Department of Law Enforcement (FDLE) regarding any ransomware incident or a cybersecurity incident level 3, 4, or 5 within 12 hours of discovery.

REPORT AN INCIDENT

FLORIDA DIGITAL SERVICE CYBERSECURITY OPERATIONS CENTER	FLORIDA DEPARTMENT OF LAW ENFORCEMENT (FDLE) CYBERCRIME OFFICE
• Email: CSOC@digital.fl.gov	• Email: CyberCrimeOffice@fdle.state.fl.us
• Phone: 850-412-6074	• Phone: 850-410-7069

FILL OUT WEB FORM

When reporting an incident you may request assistance from the Cybersecurity Operations Center, the Cybercrime Office of the Department of Law Enforcement, or the sheriff who has jurisdiction (for local governments only).



The 2024/25 Florida Local Government Cybersecurity Grant Program (Year 2)



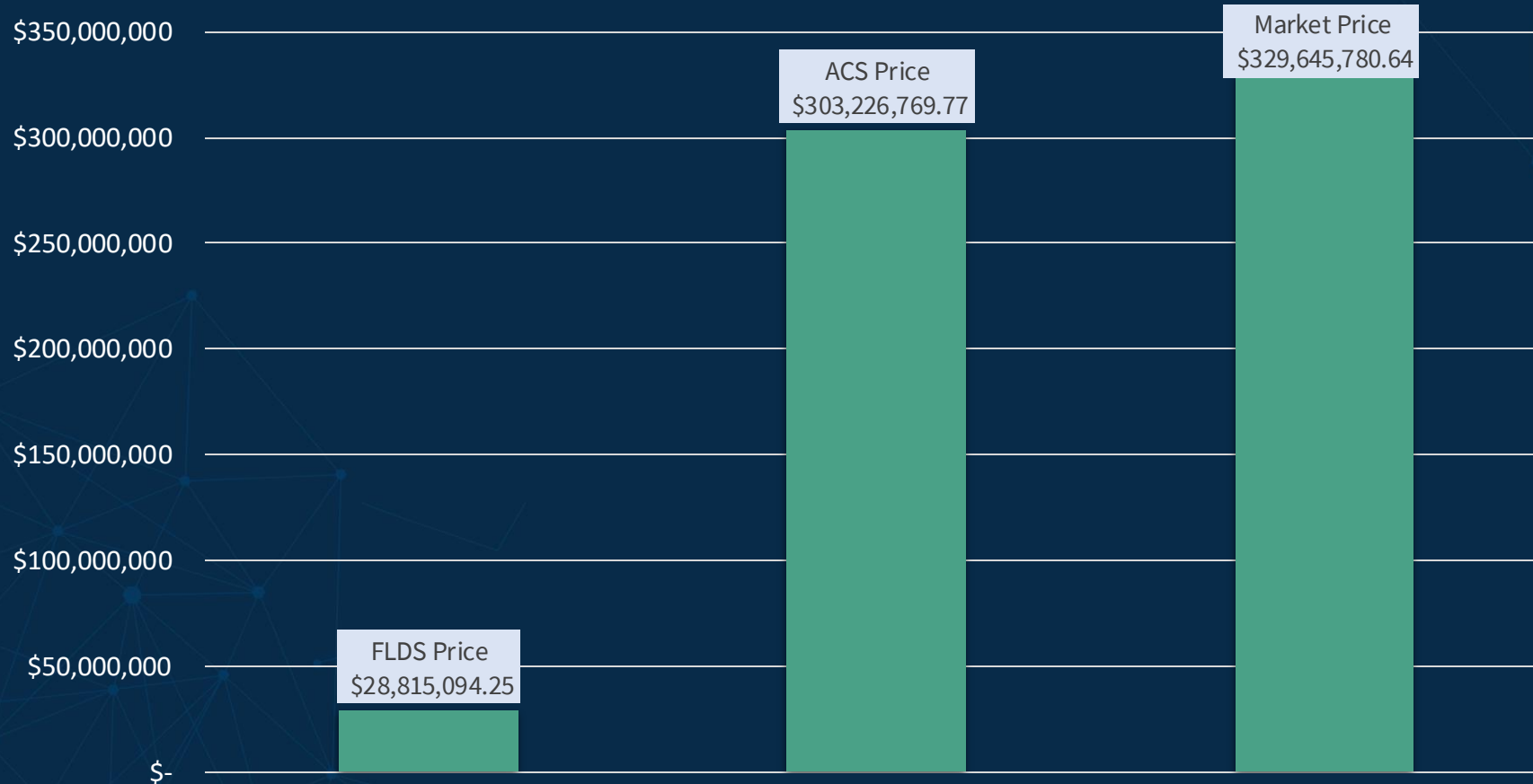
Florida Local Government Cybersecurity Grant

Florida Legislature provided \$40M for local government cybersecurity technical assistance grants for Florida Fiscal Year 2024/25.



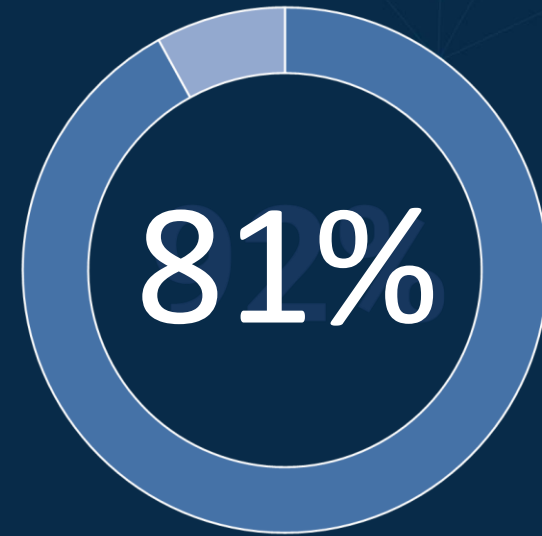
Turning a Dime into a Dollar: The FY 2022/23 Program (Year 1)

Cost Savings:



Florida Local Cybersecurity Grant Program Year 2 – Round 1

Local governments agreeing to
share threat information with CSOC
through solutions



Eligibility

- Local Governments including:
 - Board of County Commissioners
 - Cities/Mayor's Office
 - Clerks of Courts
 - First Responders (Police/Sheriff or Fire Districts)
 - Property Appraiser's Offices
 - Tax Collector's Offices
 - Infrastructure (Utility, Aviation, Port Authority, etc.)
 - Supervisor of Elections Offices
 - Special Districts



Related Provisions in Florida Statutes



Ransomware Compliance and Cybersecurity Protection

Florida Statute Section 119.0725 – Public Records Exemptions

Aligns local government with state agencies, exempting:

- Coverage limits
- Critical infrastructure information
- Network schematics, hardware and software configurations, and response practices
- Public meetings regarding exempt information

Florida Statute Section 282.3186 – Ransomware Incident Compliance

Aligns local government with state agencies, enforcing:

- Prohibition from paying or complying with ransom demands
- A robust response strategy without yielding to attackers, ensuring the security and integrity of government operations.



Florida Statute Section 112.22:

Use of applications from foreign countries of concern prohibited.

Blocking and Restricting Access:

- Mandates that any prohibited applications must be removed, deleted, or uninstalled from government-issued devices within 15 calendar days following the release or update of the prohibited applications list.
- Requires public employers to block access to and ensure the ability to remotely wipe prohibited applications from all networks and government-issued devices.
- Prohibits employees and officers of public employers from downloading or accessing any prohibited applications on government-issued devices.
- Provides exceptions for law enforcement and an exception process for other uses

Exceptions and Waivers:

- Provides exceptions for law enforcement officers if the use of the prohibited applications is necessary for public safety or conducting investigations.
- Allows public employers to request a waiver from the DMS for designated employees or officers to access prohibited applications under controlled circumstances, for a specified timeframe not exceeding one year, with potential for extension.



Prohibited Applications on Government Devices List

The Department of Management Services, through the Florida Digital Service, has determined the following applications meet the criteria for prohibited applications established in section 112.22(1)(f), Florida Statutes.

For waiver requests, please see Rule 60GG-2.008, Florida Administrative Code. If you have questions, please reach out to our team via email Policy@digital.fl.gov.

- QQ
- TikTok
- WeChat
- VKontakte
- Kaspersky

https://www.dms.myflorida.com/prohibited_applications_list



Call To Action

Your Next Steps for Cybersecurity Readiness

- Engage Your Team and Review
The Local Government Cybersecurity Packet Together
- Join Our Quarterly Meetings
- Prevention is Key: Implement Proactive Cybersecurity Measures



Taking these steps today can prevent major challenges tomorrow.



Contact Us

State CISO: CISO@digital.fl.gov

Cybersecurity: Security@digital.fl.gov



