

FL [Digital Service]

**Fiscal Year 2024/25 Florida Local Government
Cybersecurity Grant Webinar**

March 29, 2024



Welcome & Introductions

Thanks for joining us!

This webinar will provide information on Round 1 of the Florida Local Government Cybersecurity Grant, the application process, the timeline, and an overview of this year's process.



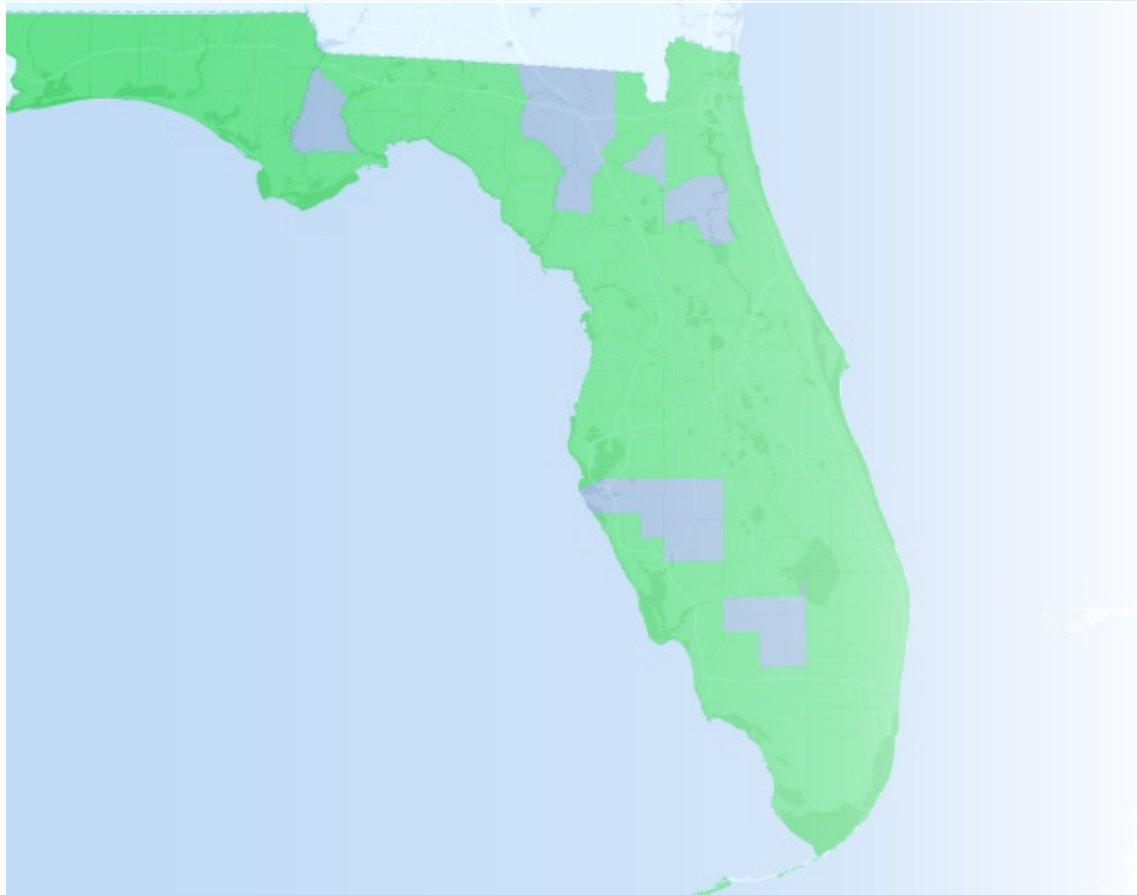
About FL[DS] - Cyber

FL[DS] serves as the lead state entity on cybersecurity. Florida Statute sections 282.318 & 282.3185 direct the Digital Service to:

- Operate and maintain a **Cybersecurity Operations Center** led by the State CISO
- Detect threats through data correlation, **continuous security monitoring**, and defined detection processes.
- Establish incident response teams to **provide incident response support** to state and local governments upon request.



The FY 2022/23 Program

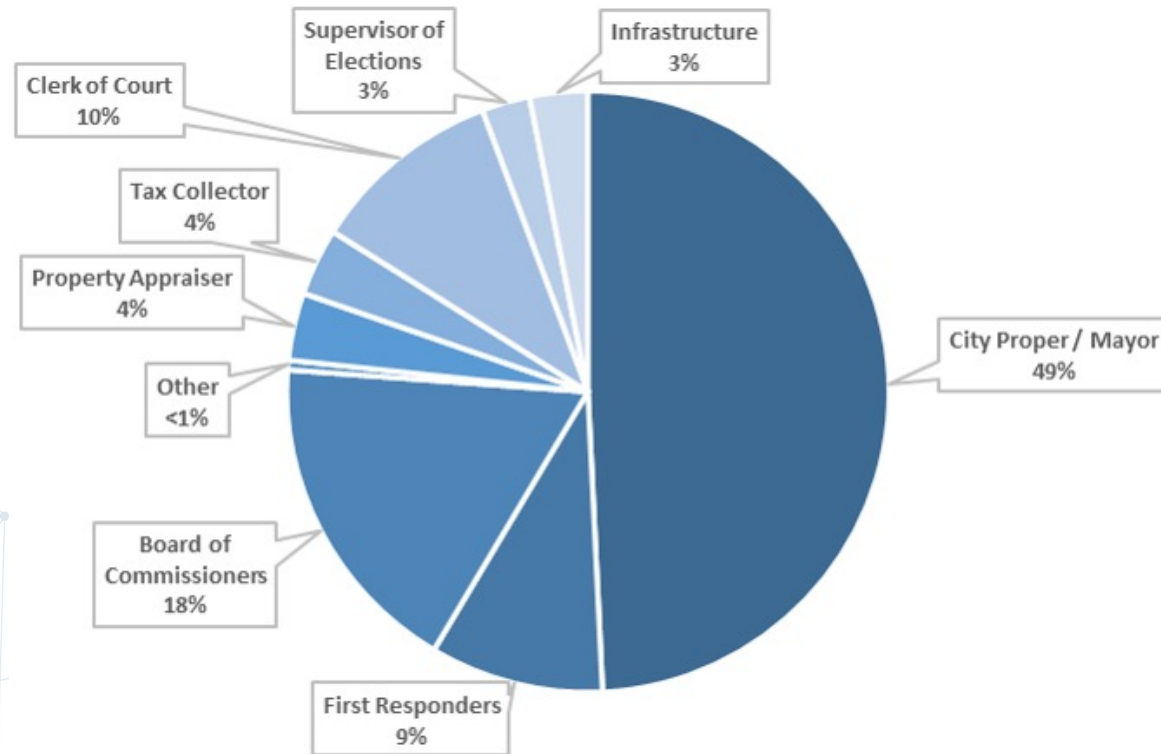


- Grants were **awarded to 193 local government** entities across the state.
- Included recipients from **56 of the 67 Florida counties**.
- **736 solutions** were awarded across **7 different capabilities**.
- Over **96 percent of awardees** agreed to share telemetry data with the CSOC.



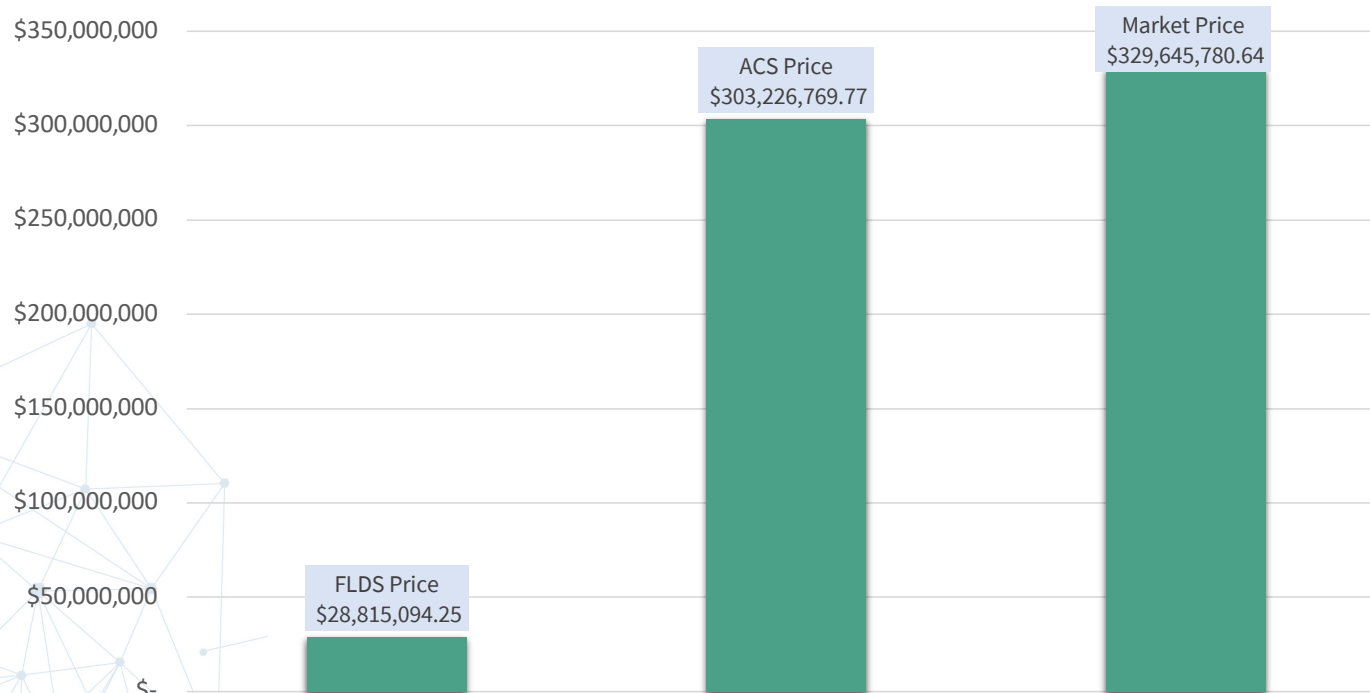
The FY 2022/23 Program

Local Government Type Distribution:



The FY 2022/23 Program

Cost Savings:





The 2024/25 Florida Local Government Cybersecurity Grant Program



Florida Local Government Cybersecurity Grant

Florida Legislature provided \$40M for local government cybersecurity technical assistance grants for Florida Fiscal Year 2024/25. Funding is contingent upon approval of the 2024/25 budget.

Two Rounds:

- Round 1 allows local governments the option to apply for cybersecurity capabilities that are currently implemented and operational within their environments.
 - Accelerated timeframe to minimize any gaps in service.
 - Limited to quantity changes for implemented services.

Any new capability requests will be separated from round 1 and included in the round 2 process.

- Round 2 allows for allows local governments new to the program, or existing grantees the option of applying for new cybersecurity capabilities or changing providers.



Florida Local Government Cybersecurity Grant

Highlights:

- Easy to apply. No narrative requirement; no justifications, no critiques. We collect only what we need for selection criteria and to connect you with the right capabilities.
- You are provided with top-tier capabilities without the headaches of procurement, follow-on audits, and vendor management.
- Optional integration with the state Cybersecurity Operations Center allows for rapid Incident Response support when requested and detection and monitoring services baked-in.
- All capabilities come with both implementation and support services where needed.



Florida Local Government Cybersecurity Grant

What is Different this Year:

- Will be able to leverage much of the work products from last year.
- An updated approach to communications management to ensure emails are handled quickly and completely.
- Based on your feedback, improved planning, structure, and upfront communication to provide you clearer expectations and a smoother process.
- Overall, we look to provide a more organized and responsive grant program this year.



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

- Round 1

- Local Governments who are grant recipients and have capabilities deployed in their environment.

- Round 2

- Local Governments who are not grant recipients or are grant recipients but wish to add capabilities or change from one provider to another.



Offered Capabilities

- **External-Facing Asset Discovery:** This capability identifies digital assets accessible from the internet, helping the state assess potential entry points for cyber threats and vulnerabilities.
 - Palo Alto Xpanse
 - Tenable.ASM
- **Endpoint-Based Asset Discovery:** By detecting devices connected to the network, this capability aids in maintaining an up-to-date inventory of hardware, improving security management and incident response.
 - N-Central
 - Tanium Asset Disc
- **Network-Based Asset Discovery:** Focuses on identifying devices from a network perspective, helping administrators gain visibility into all network-connected assets.
 - Armis
 - Netskope
 - Tenable.IO
- **Email Security Gateway:** Protecting against email-based threats, this capability filters incoming emails for malicious content, shielding communication channels from phishing and malware.
 - Abnormal
 - Cisco
 - Proofpoint

- **Security Operations Platform:** Centralizing security operations, this platform enables continuous monitoring, threat detection, and coordinated incident response across digital infrastructure.
 - CrowdStrike SOP
 - ReliaQuest
 - Tanium SOP
 - Tenable.ONE
 - Secureworks
 - Chronicle Sec Ops (Google-Core)
- **Endpoint Protection and Response:** This capability safeguards individual devices from cyber threats by preventing, detecting, and responding to malicious activities in real-time.
 - Cisco EDR
 - CrowdStrike EDR
 - Fortinet EDR
 - Palo Alto EDR
 - SentinelOne
 - VMware Carbon Black
- **Content Delivery Network:** By distributing web content across a network of servers, this capability enhances website performance and provides security against various online threats.
 - Akamai
 - Cloudflare



Grant Process



Timeline

- Application opens for Round 1 and Round 2 the first week of April
- Application window closes for Round 1 on April 26th, 2024
- Awards and grant agreements issued week of May 6th, 2024
- Grant agreements returned to FL[DS] – by June 21st, 2024
- Grant agreements executed by July 1st, 2024
- Purchase orders executed by early July, 2024
- Round 2 processing begins
- Round 2 capabilities deployed early 2025



Florida Local Government Cybersecurity Grant

Our Approach:

- We believe that cybersecurity is a team sport. We strive to enable your teams with tools that make a difference in the fight against cyber crime.
- The FL[DS] follows and will adhere to the principle of least privilege. FL[DS] will only have access to the specific data, resources, and applications needed to enable your organization with the agreed upon capabilities you request and are awarded.
- Your organization will maintain ownership, management, and administrative rights of your environment and the components within this program.
- We are committed to cyber readiness and posturing the state to defend against threats, respond rapidly to incidents, and recover as quickly as possible so you can continue serving the citizens and communities of Florida.



What to do first

- Apply at Cybergrants.fl.gov
- Start reviewing and shopping around the following documents to clear the way for any signatures (like Grant Agreement) you need to obtain.
 - Grant Agreement
 - Data Sharing Agreement
 - Incident Response Rider
 - Software Specific Riders (as needed)
 - Warranties and Commitments
- Monitor your email and Cybergrants.fl.gov for updates and communications regarding your application.



Questions?

Helpful resources

- Email inbox: CyberSecurityGrants@digital.fl.gov
- Application: CyberGrants.fl.gov

Issues?

- Please let us know and give us the opportunity to make it right.

