Florida Local Government Cybersecurity Grant Application Aide

This application aide is designed to assist you by identifying the information you will need to collect to submit an official grant application through the online grants form. This document will **not be accepted** as a grant application.

The Department of Management Services, acting through the Florida Digital Service (FL[DS]), is the lead entity responsible for establishing standards and processes for assessing state agency cybersecurity risks and determining appropriate security measures in the state of Florida (s. 282.318, Florida Statutes).

Pursuant to section 282.3185(4), Florida Statutes, each local government shall adopt cybersecurity standards that safeguard its data, information technology, and information technology resources to ensure availability, confidentiality, and integrity. Dates for local government adoption of the cybersecurity standards and required notification to the FL[DS] of its compliance are also defined in section 282.3185(4), Florida Statutes.

The FL[DS] is administering the Florida Local Government Cybersecurity Grant Program to provide assistance to Florida Local Governments for the development and enhancement of cybersecurity risk management programs. This program is funded for the 2024/25 State of Florida fiscal year; however, it is contingent upon funding approval and release. Future funding for this program is subject to legislative appropriation.

* Denotes required information

ORGANIZATION/APPLICANT INFORMATION

*Organization Name:

*Organization Type (City, County, Clerk of Court, Property Appraiser, Sheriff's Office, Supervisor of Elections, Tax Collector, Special District, Authority, *Other*)

*If *Other*, Describe Organization Type: *Organization County:

*Mailing Address:

*City: *Zip Code:

*Main Website Address:

Executive Sponsor for Grant:

*Name: *Title:

*Primary Phone Number:

Secondary Phone Number:

*Email Address

Primary Contact for Grant:

*Name: *Title:

*Primary Phone Number:

Secondary Phone Number:

*Email Address

Additional Contacts - Information Technology Director:

Name:

Title:

Primary Phone Number:

Secondary Phone Number:

Email Address

Additional Contacts - Chief Information Security Officer or Security Manager:

Name:

Title:

Primary Phone Number:

Secondary Phone Number:

Email Address

Additional Contacts – Primary Contact for Coordination of Cybersecurity Incidents:

Name:

Title:

Primary Phone Number:

Secondary Phone Number:

Email Address

ABOUT YOUR ORGANIZATION:

*Total number of supported users (Staff, Contractors):

Total number of staff members dedicated to cybersecurity (Employees and Contractors):

*Annual operating budget of organization:

Total budget for cybersecurity:

*Total number of physical sites/locations:

Local Eligibility:

*Is your organization funded or its budget approved by a county or municipality? (Y/N)

*Is your organization governed by a county or municipality? (Y/N)

*Is your organization governed by locally elected officials? (Y/N)

Are there other reasons your organization is considered to be a local entity? If so, please explain them:

ABOUT YOUR INFORMATION TECHNOLOGY ENVIRONMENT:

Does your entity provide constituent/public facing applications? (Y/N)

If Yes, how many constituents/members of the public do you serve?

*Does your organization manage critical infrastructure as defined by rule 60GG-2.001(2)(a)10, F.A.C. or s. 692.201, Florida Statutes? (Y/N)
60GG-2.001(2)(a)10, F.A.C. | s. 692.201, Florida Statutes

If Yes:
*How many sites/locations include critical infrastructure?

Provide any additional information regarding critical infrastructure as it pertains to this grant application:

*Total number of supported endpoints/devices (e.g. laptops, desktops, servers, mobile devices)?

Date of your most recent cybersecurity risk assessment?

What is your biggest motivation(s)/ reason(s) to apply for this grant opportunity?

FLORIDA CYBERSECURITY PROGRAM PARTICIPATION

*Are you a current awardee and active participant in the Florida Local Government Cybersecurity Program? (Y/N)

*If Yes, please provide your grant agreement number.

*Have you or do you have plans for the near future to participate in the Florida Critical Infrastructure Risk Assessment? (Y/N)

*Are there state cybersecurity laws or rules you are out of compliance with and require financial assistance for remediation? (Y/N)

*If Yes, please explain.

INTEGRATION WITH STATE CYBERSECURITY OPERATIONS CENTER (CSOC)

The State CSOC is designed to serve as a single point of ingestion for cybersecurity data and provides a multi-tenant framework that allows for relevant data sharing while preserving the sovereignty of participating entities. This data is used to monitor and detect threats across Florida's cybersecurity landscape.

*Are you willing to integrate solutions provided through this grant into the Cybersecurity Operations Center? (Y/N)

OUR COMMITMENTS TO YOU

The FL[DS] is committed to least privileged access because we believe in privacy and the minimum access required to administer the offered cyber capabilities and incident response, when requested. The following agreements will be delivered as two-party agreements with FL[DS] and your organization. They clearly describe the Florida Digital Service's intent, limitations, and restrictions. These signed agreements between FL[DS] and your organization are required within 30 days after award and prior to any solution implementation. Example riders and agreements can be found on the main Local Government Cybersecurity Grant Program webpage under the "Additional Resources" section.

- Grant Agreement
- Grantee Data Sharing Agreement
- Incident Response Rider
- Software Rider(s) as needed

Commitments document will be included as part of the post-award process and provide important assurances to your organization regarding this grant.

CYBERSECURITY CAPABILITIES

Please tell us about the following cybersecurity capabilities as it pertains to your IT environment and if you are requesting these capabilities for your organization as part of this grant opportunity. If you have questions about any of these capabilities, please contact cybersecuritygrants@digital.fl.gov.

Endpoint-Based Asset Discovery - A solution focused on infrastructure which discovers network connected devices and provide a comprehensive inventory of hardware and software assets across your enterprise. Agents are typically deployed to all laptop, desktop, and server devices.

*Are you requesting Endpoint-Based Asset Discovery capabilities through this grant opportunity? (Y/N)

If Yes Requesting:

*Do you have a solution providing this capability deployed in your environment and if so, are you currently receiving it through the Florida Digital Service? (Yes, through FL[DS]/Yes, not through FL[DS]/No)

If Yes has Solution:

*Percentage of your assets (Windows, Linux, MacOS) covered by this solution (if yes):

*Name of the solution(s) you have deployed (if yes):

*Provider and product/service name of your preferred solution for this year's grant:
Select one: (NCentral, Tanium, No Preference)

*How many computer users will be covered by this capability?

*How many devices in your environment (Windows, Linux, & MacOS) will be covered by this capability?

*When is the soonest your organization will be ready to start implementing this capability from date of award?
Select one: (currently implemented, less than 30 days, 31-60 days, 61-90 days, 91-120 days, longer)

Network-Based Asset Discovery – A solution providing enterprise visibility into managed, unmanaged and Internet of Things (IoT) devices discovered via network traffic.

*Are you requesting Network-Based Asset Discovery capabilities through this grant opportunity? (Y/N)

If Yes Requesting:

*Do you have a solution providing this capability deployed in your environment and if so, are you currently receiving it through the Florida Digital Service? (Yes, through FL[DS]/Yes, not through FL[DS]/No)

If Yes has Solution:

*Percentage of your assets covered by this solution (if yes):

*Name of the solution(s) you have deployed (if yes):

*Provider and product/service name of your preferred solution:
Select one: (Armis, Netskope IoT Security, Tenable.IO, No Preference)

*How many physical locations (local area networks) will be covered by this capability?

*Total number of computer users in organization (include all employment types):

*When is the soonest your organization will be ready to start implementing this capability from date of award?
Select one: (currently implemented, less than 30 days, 31-60 days, 61-90 days, 91-120 days, longer)

External-Facing Asset Discovery - An internet-facing attack surface discovery tool which provides a continuously updated inventory and vulnerability scanning of all global internet-facing assets to detect on-premises and cloud systems.

*Are you requesting Internet-Facing Asset Discovery capabilities through this grant opportunity? (Y/N)

If Yes Requesting:

*Do you have a solution providing this capability deployed in your environment and if so, are you currently receiving it through the Florida Digital Service? (Yes, through FL[DS]/Yes, not through FL[DS]/No)

If Yes has Solution:

*Percentage of your external-facing assets covered by this solution (if yes):

*Name of the solution(s) you have deployed (if yes):

*Provider and product/service name of your preferred solution:
Select one: (Palo Alto Networks Xpanse, Tenable Attack Surface Management, No Preference)

*How many external-facing assets are in your environment (publicly advertised IP addresses)?

*When is the soonest your organization will be ready to start implementing this capability from date of award?
Select one: (currently implemented, less than 30 days, 31-60 days, 61-90 days, 91-120 days, longer)

Content Delivery Network – Software, including web application firewall, to manage and secure enterprise websites and APIs against DDos and targeted web app attacks while fending off adversarial bots and detecting client-side script attacks.

*Are you requesting Content Delivery Network capabilities through this grant opportunity? (Y/N)

If Yes Requesting:

*Do you have a solution providing this capability deployed in your environment and if so, are you currently receiving it through the Florida Digital Service? (Yes, through FL[DS]/Yes, not through FL[DS]/No)

If Yes has Solution:

*Percentage of your hostnames covered by this solution (if yes):

*Name of the solution(s) you have deployed (if yes):

*Provider and product/service name of your preferred solution:
Select one: (Akamai, Cloudflare, No Preference)

*Number of endpoints (Windows, Linux, MacOS) within your organization:

*When is the soonest your organization will be ready to start implementing this capability from date of award?
Select one: (currently implemented, less than 30 days, 31-60 days, 61-90 days, 91-120 days, longer)

Endpoint Detection & Response (EDR) - An agent deployed to each endpoint (including desktops, laptops, and servers), runs autonomously on each device and monitors all processes in real-time to provide enterprise visibility, analytics, malware defense, and automated response.

*Are you requesting Endpoint Protection & Response (EDR) capabilities through this grant opportunity?

If Yes Requesting:

*Do you have a solution providing this capability deployed in your environment and if so, are you currently receiving it through the Florida Digital Service? (Yes, through FL[DS]/Yes, not through FL[DS]/No)

If Yes has Solution:

*Percentage of your assets (Windows, Linux, MacOS) protected by this solution (if yes):

*Name of the solution(s) you have deployed (if yes):

*Provider and product/service name of your preferred solution for this year's grant (if you have a preference):
Select one: (Carbon Black, Cisco Secure Endpoint, CrowdStrike, Fortinet FortiEDR, Palo Alto Cortex Endpoint Protection, SentinelOne, No Preference)

*How many devices in your environment (Windows, Linux, MacOS) will be protected by this capability?

*When is the soonest your organization will be ready to start implementing this capability from date of award?
Select one: (currently implemented, less than 30 days, 31-60 days, 61-90 days, 91-120 days, longer)

Email Security – Protects your email accounts from threats such as phishing attacks and malware.

*Are you requesting Email Security capabilities through this grant opportunity? (Y/N)

If Yes Requesting:

*Do you have a solution providing this capability deployed in your environment and if so, are you currently receiving it through the Florida Digital Service? (Yes, through FL[DS]/Yes, not through FL[DS]/No)

If Yes has Solution:

*As a percentage, how complete is your implementation of this solution (if yes)?

*Name of the solution(s) you have deployed (if yes):

*Provider and product/service name of your preferred solution for this year's grant:
Select one: (Abnormal, Cisco Secure Email, Proofpoint, No Preference)

*Total number of named email accounts within organization (exclude shared mailboxes):

*Total number of computer users in organization (include all employment types):

*When is the soonest your organization will be ready to start implementing this capability from date of award?
Select one: (currently implemented, less than 30 days, 31-60 days, 61-90 days, 91-120 days, longer)

Security Operations Platform - Providing 24/7/365 monitoring and initial incident investigations to augment your security team.

*Are you requesting Security Operations Platform capabilities through this grant opportunity? (Y/N)

If Yes Requesting:

*Do you have a solution providing this capability deployed in your environment and if so, are you currently receiving it through the Florida Digital Service? (Yes, through FL[DS]/Yes, not through FL[DS]/No)

If Yes has Solution:

*As a percentage, how complete is your implementation of this solution (if yes)?

*Name of the solution(s) you have deployed (if yes):

*Provider and product/service name of your preferred solution for this year's grant:
Select one: (Google Chronicle SecOps, CriticalStart, CrowdStrike, Foresite, Reliaquest GreyMatter, SecureWorks XDR, Tanium SOP, Tenable.ONE, No Preference)

*Total number of staff members in organization (include all employment types):

*When is the soonest your organization will be ready to start implementing this capability from date of award?
Select one: (currently implemented, less than 30 days, 31-60 days, 61-90 days, 91-120 days, longer)

ADDITIONAL CYBERSECURITY CAPABILITY NEEDS

Please tell us about other capabilities/ solutions that you would like to see offered, the provider, and product/service name of your preferred solution (if you have a preference). Check all that apply:

	Capability:	Provider and Preferred Product/Service Name:
□	Multi-Factor Authentication (MFA)	
□	Business Continuity (backup, disaster recovery)	
□	Identity and Access Management	
□	Private Access / Secure (Access) Service Edge	
□	Security Information Event Management	
□	Governance, Risk and Compliance	
□	Investigation, Visualization and Reporting	
□	Vulnerability Assessment and Management	
□	Cybersecurity Risk Assessment Services	
□	Cybersecurity Consulting Services	
□	Other:	*Describe other capability desired:

GRANT MATCHING

*If awarded through the Florida Local Cybersecurity Grant Program, do you plan to seek funding outside of the grant program (whether through your organization's budget or seeking other funding opportunities) to continue awarded solutions? (Y/N)

If Yes:

*When would you anticipate assuming the fiscal responsibility? (CY2024/CY2025/CY2026):

*What percentage of awarded value would you anticipate assuming that year? (10-100):

ADDITIONAL INFORMATION

If you have additional information to share regarding your application, including justification, ability to provide matching funds/continued funding, explanation of needs, information on critical infrastructure, environmental factors, state resiliency or any other relevant information, please provide below or upload the information in the attachments section labeled as Additional Information.

📎 *Additional Information Attachments*