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 portal. This document will **not be accepted** as a grant application.

Florida Local Government Cybersecurity Grant Program

The Florida Digital Service (FL[DS]) is the lead entity for cybersecurity in the state of Florida. It is responsible for establishing safeguards to protect data, responding to cybersecurity incidents, assessing cybersecurity risk and maturity, and developing necessary cybersecurity standards and frameworks.

The FL[DS] is administering the Florida Local Government Cybersecurity Grant Program, a competitive program to extend the cybersecurity capabilities of the FL[DS] Cybersecurity Operations Center (CSOC) to Florida municipal and county governments to improve their cybersecurity posture and resiliency.

* Denotes required information unless not applicable

ORGANIZATION/APPLICANT INFORMATION

*Organization Name:	*Organization Type (Municipality, County)
*Organization Subtype (Mayor, Board of Commissioners, Clerk of Court, Property Appraiser, Sheriff's Office, Supervisor of Elections, Tax Collector, *Other*)	
*If *Other* Subtype:	*Organization County:
*Mailing Address:	
*City:	*Zip Code:
*Main Website Address:	*Tax ID:

Executive Sponsor for Grant:

*Name:	Title:
*Office Phone Number:	*Receive texts? (Y/N)
Mobile Phone Number:	Receive texts? (Y/N)
*Email Address	

Primary Contact for Grant:

*Name:	*Title:
*Office Phone Number:	*Receive texts? (Y/N)
Mobile Phone Number:	Receive texts? (Y/N)
*Email Address	

Additional Contacts - Information Technology Director:

Name:	Title:
Office Phone Number:	Receive texts? (Y/N)
Mobile Phone Number:	Receive texts? (Y/N)
Email Address	

Additional Contacts - Chief Information Security Officer or Security Manager:

Name:	Title:
Office Phone Number:	Receive texts? (Y/N)
Mobile Phone Number:	Receive texts? (Y/N)
Email Address	

ABOUT YOUR ORGANIZATION:

Total number of supported users (Customers, Staff, Contractors, Students):

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)

Are your organization's systems or data integrated with those of a county or municipality? (Y/N)

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

ABOUT YOUR IT ENVIRONMENT:

Does your infrastructure send data across My Florida Network MFN2? (Y/N)

Do any of your network(s) send or receive data to/from infrastructure or applications hosted by the State of Florida? (Y/N)

Do the employees of your organization use applications provided by the State of Florida? (Y/N)

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

How many constituents/members of the public do your applications serve annually?

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

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?

REQUESTED DOCUMENTATION

To align your organization with the right capabilities and to be better prepared to support you when responding to an incident, the following documents are requested post award. Which of these documents is your organization willing to consider sharing with the FL[DS], subject to the protections of 119.0725, F.S.?

*Network Diagrams (Y/N)

*Critical Systems Inventory (Y/N)

*Critical Infrastructure Inventory (if applicable) (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

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

FUTURE CYBERSECURITY CAPABILITY NEEDS

To help us plan for future grant program offerings should they become available, 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:

		Provider:	Preferred Product/Service Name:
☐	Multi-Factor Authentication (MFA)		
☐	Application Dependency and Performance Monitoring		
☐	Business Continuity (backup, disaster recovery, data encryption)		
☐	Identity and Access Management		
☐	Centralized Ticketing and Asset Management		
☐	Private Access / Secure (Access) Service Edge		
☐	Security Event Information Management		
☐	Governance, Risk and Compliance Tool		
☐	Investigation, Visualization and Reporting Tool		
☐	Email Security Service or Solution		
☐	Vulnerability assessment and management tool		
☐	Other:		

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.

*Do you have a solution providing this capability deployed in your environment? (Y/N)

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

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

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

If Yes:

Provider and product/service name of your preferred solution (if you have a 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: (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.

*Do you have a solution providing this capability deployed in your environment? (Y/N)

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

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

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

If Yes:

Provider and product/service name of your preferred solution (if you have a preference):

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

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: (less than 30 days, 31-60 days, 61-90 days, 91-120 days, longer)

External-Facing Asset Discovery - A web-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.

*Do you have a solution providing this capability deployed in your environment? (Y/N)

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

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

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

If Yes:

Provider and product/service name of your preferred solution (if you have a preference):

How many external-facing assets are in your environment?

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

Content Delivery Network - Software to manage and secure enterprise web and mobile assets, both .com and .gov, by protecting websites and APIs against DDoS and targeted web app attacks while fending off adversarial bots, detecting client-side script attacks, and protecting your users' accounts from fraud.

*Do you have a solution providing this capability deployed in your environment? (Y/N)

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

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

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

If Yes:

Provider and product/service name of your preferred solution (if you have a preference):

Number of hostnames/domain names in your environment:

Percentage of your hostnames that will be protected by this capability:

Total estimated monthly web traffic (ex. 50GB):

*When is the soonest your organization will be ready to start implementing this capability from date of award?
Select one: (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, and automated response.

*Do you have a solution providing this capability deployed in your environment? (Y/N)

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

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

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

If Yes:

Provider and product/service name of your preferred solution (if you have a 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: (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 staffing.*

*Do you have a solution providing this capability deployed in your environment? (Y/N)

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

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

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

If Yes:

Provider and product/service name of your preferred solution (if you have a preference):

Log volume per day (in GB) to be consumed by Cyber Security Operations Center (if known):

List of Unique Log Sources and providers to be consumed (Ex: Firewall, Antivirus, Web Proxy, Etc.) that are not included in the capabilities offered by this grant opportunity:

How many devices in your environment (Windows, Linux, MacOS):

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

ADDITIONAL NEEDS

If there are cybersecurity capabilities specific to your organization you would like us to consider, please provide information about the need and its criticality, the solution and its projected impact, the estimated cost, and how you would procure, manage, and integrate the solution with the State Cybersecurity Operations Center. Provide sufficient information to establish goals for award and to demonstrate performance post-award. You may upload any supporting documentation in the attachments section labeled as Additional Needs.

_____

_____

Additional Needs Attachments

ADDITIONAL INFORMATION

If you have additional information to share regarding your application including justification, 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