Agenda Item #3K-2

PALM BEACH COUNTY
BOARD OF COUNTY COMMISSIONERS

AGENDA ITEM SUMMARY

Meeting Date: **August 19, 2025** **Consent [X]** **Regular [ ]**
Public Hearing [ ]

Department: **Water Utilities Department**

I. EXECUTIVE BRIEF

Motion and Title: Staff recommends motion to:

A.) authorize the Palm Beach County Water Utilities Department (PBCWUD) to pursue funding from the following two (2) sources:

1. Florida Department of Environmental Protection (FDEP) Resilient Florida Grant Program for a combined grant amount estimated up to $60,000,000 for three Water Treatment Plant (WTP) Nos. 2, 8 and 11 (Projects);

2. Department of Management Services (DMS) through Florida Digital Service (FDS) for the Local Government Cybersecurity Grant Program assistance in the amount of $500,000; and

B.) delegate authority to the County Administrator, or designee, to sign all grant application forms and supporting documents and complete all registration requirements, execute the forthcoming grant agreement and all future time extensions, task assignments, certifications, and other forms associated with the forthcoming grant agreement and any necessary minor amendments that do not substantially change the scope of work, terms, or conditions of the forthcoming grant agreement.

Summary: FDEP has allotted funding for fiscal year 2025-26 for the Resilient Florida Grant Program to effectively address the impacts of flooding and sea level rise that the state faces through projects that analyze and plan for vulnerabilities and implementation projects for adaptation and mitigation. Grant applications are due to FDEP on September 1, 2025. PBCWUD has a comprehensive plan for future upgrades to WTP Nos. 2, 8 and 11, which will contribute to regional resiliency efforts and increase reliability for hurricanes. PBCWUD is seeking grant funding to defray costs as it continues its efforts to improve infrastructure resiliency for water treatment facilities throughout the County. These measures will minimize damage, facilitate faster recovery for affected communities and reduce overall costs associated with flooding. The FDS has funds available for fiscal year 2025-2026 to provide cybersecurity technical assistance and capabilities to Florida's local governments and to improve their cybersecurity posture and resiliency. FDS will expend funds for the provision of services, licenses, and/or commodities to enhance cybersecurity framework, to identify and mitigate risks, and to protect infrastructure from threats. Grant applicants are due to FDS on August 31, 2025. **The FDEP grant requires a 50% match, which will be funded from a one (1)-time expenditure from Water Utilities user fees, connection fees and balance brought forward.** Districts 2, 3 & 6 (MWJ)

Background and Justification: (Continued on page 3)

Attachments:

1. FDEP Resilient Florida Grant Program Request for Applications
2. DMS Local Government Cybersecurity Grant Program Request for Applications

Recommended By: ______________________ 7/17/25
Department Director **Date**

Approved By: ______________________ 8/2/25
Assistant County Administrator **Date**

II. FISCAL IMPACT ANALYSIS

A. Five Year Summary of Fiscal Impact:

Fiscal Years	2025	2026	2027	2028	2029
Capital Expenditures	0	0	0	0	0
Operating Costs	0	0	0	0	0
External Revenues	0	0	0	0	0
Program Income (County)	0	0	0	0	0
In-Kind Match County	0	0	0	0	0
NET FISCAL IMPACT	$0	0	0	0	0
# ADDITIONAL FTE POSITIONS (Cumulative)	0	0	0	0	0

Budget Account No.: **Fund** **Dept.** **Unit** **Object**

Is Item Included in Current Budget? Yes ____ No ____

Does this item include the use of federal funds? Yes____ No ____

Is this item using State Funds? Yes ____ No ____

Reporting Category **N/A**

B. Recommended Sources of Funds/Summary of Fiscal Impact:

No Fiscal Impact

C. Department Fiscal Review: Ebony Foreman

III. REVIEW COMMENTS

A. OFMB Fiscal and/or Contract Development and Control Comments:

Lisa Mart 7/22/2025
OFMB JA 7/21
DA 7/21
MF 7/22

Brenda Znachko
Contract Development and Control
RG 7.23.25
OD 7.24.25

B. Legal Sufficiency:

7/24/25
Assistant County Attorney

C. Other Department Review:

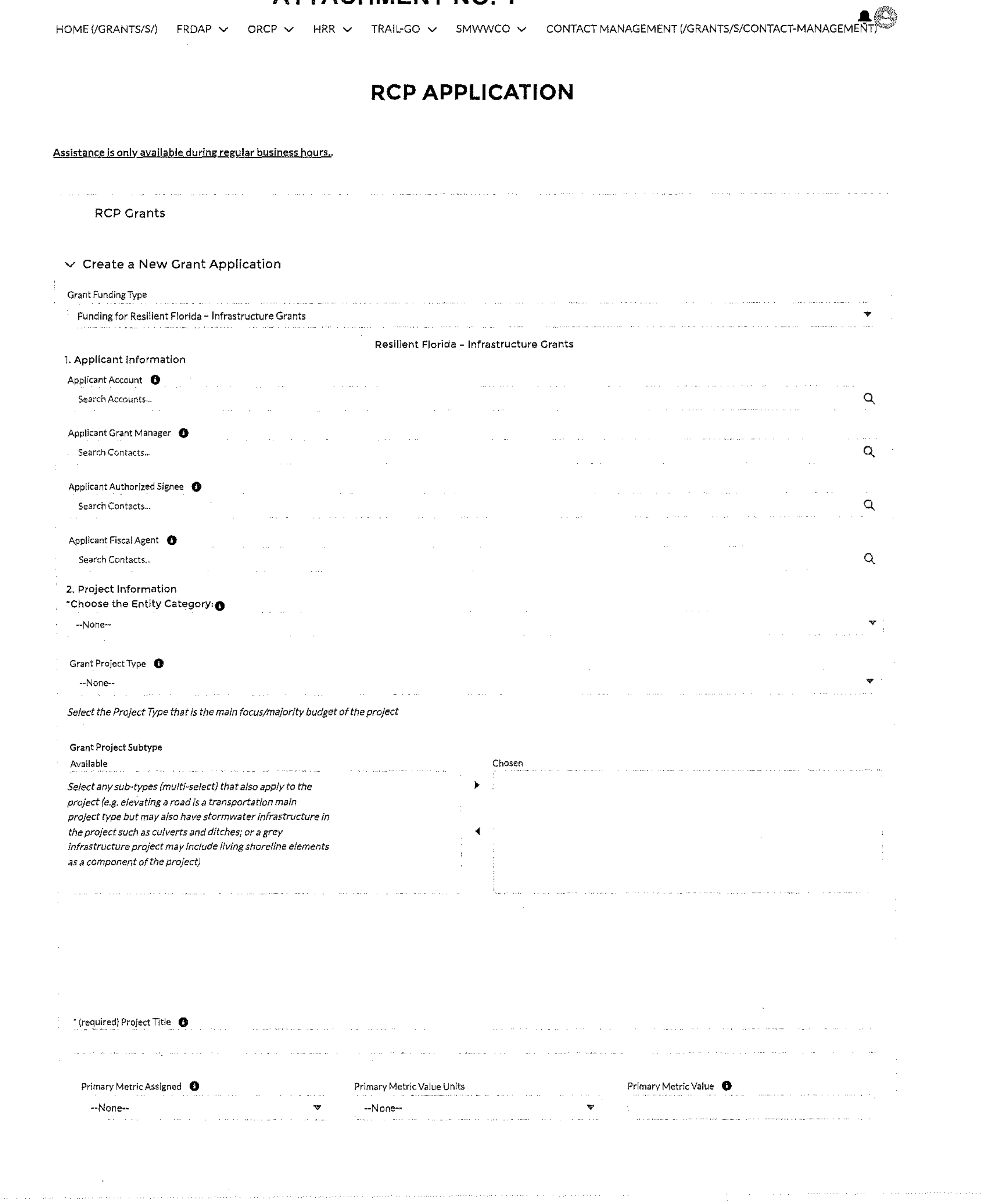
____
Department Director

This summary is not to be used as a basis for payment.

Continued from page 1.

Background and Justification: On May 12, 2021, Governor Ron DeSantis signed Senate Bill 1954 into law that allocates funding to support a coordinated approach to Florida's coastal and inland resiliency. The Resilient Florida Program aids efforts to protect inland waterways, coastlines and shores, which serve as natural defenses against sea level rise, as well as, prepare communities for the impacts of climate change – including sea level rise, intensified storms, flooding, and inland mitigation. The improvements contained in the Projects will ensure cost savings, better health outcomes and reduced environmental impact for the County. FDS has allotted $15 million for fiscal year 2025-2026 to local governments to enhance cybersecurity resilience. This grants aids PBCWUD's efforts to enhance security and mitigation strategies.

ATTACHMENT NO. 1



RCP APPLICATION

Assistance is only available during regular business hours..

RCP Grants

Create a New Grant Application

Grant Funding Type

Funding for Resilient Florida - Infrastructure Grants

Resilient Florida - Infrastructure Grants

1. Applicant Information

Applicant Account

Search Accounts...

Applicant Grant Manager

Search Contacts...

Applicant Authorized Signee

Search Contacts...

Applicant Fiscal Agent

Search Contacts...

2. Project Information

*Choose the Entity Category:

--None--

Grant Project Type

--None--

Select the Project Type that is the main focus/majority budget of the project

Grant Project Subtype

Available

Select any sub-types (multi-select) that also apply to the project (e.g. elevating a road is a transportation main project type but may also have stormwater infrastructure in the project such as culverts and ditches; or a grey infrastructure project may include living shoreline elements as a component of the project)

Chosen

* (required) Project Title

Primary Metric Assigned

--None--

Primary Metric Value Units

--None--

Primary Metric Value

Secondary Metric Assigned	Secondary Metric Value Units	Secondary Metric Value
--None-- ▾	--None-- ▾	

Project Location

Project Geo Location ❶

Latitude	Longitude

*Project Location Address ❶

Sponsor City/County ❶

--None-- ▾

List the City(ies)/ Town(s)/Village(s) ❶

Will any of the work to be performed, or fall on state lands? ❶ --None-- ▾

2A. General Information

⌄ Background

Project Description ❶

2B. Project Scoring Criteria

› Tier 1 Criteria Information

› Tier 2 Criteria Information

› Tier 3 Criteria Information

› Tier 4 Criteria Information

› Additional Information

› Multiagency Information

Cancel Save

› Existing Applications

ATTACHMENT NO. 2

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 2025/26 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

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: (Axonius Cybersecurity Asset Management, BlueVoyant Platform Bundle, (MDR, SIEM and Vulnerability Scanning), CrowdStrike Falcon Discover, Divergent Endpoint Asset Discovery, Elastic, Skyline Endpoint-Based Asset Discovery Services and Technology, Forescout Technologies Inc., Fortinet FortiClient/EMS FortiNAC, Heimdal Advanced Vulnerability Management Solution, Ivanti, LevelBlue USM, Lumen Manage Cybersecurity Asset Management, N-able N-central Remote Monitoring and Management (RMM), Netwatch.ai, Omnissa Workspace ONE, Open Text, Corp., SentinelOne - Singularity Vulnerability Management, SEPIO, Tanium, Tenable.IO - Vulnerability Management, Trend Micro Vision One Attack Surface Risk Management (ASRM), 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: (Akamai Technologies, Armis Centrix, Axonius Cybersecurity Asset Management, BlueVoyant Standard

Vulnerability Scanning, Check Point Infinity Network Detection and Response (NDR), Cisco Identity Services Engine (ISE), Darktrace/NETWORK, Divergent Network-Based Asset Discovery, ExtraHop Networks, Inc. RevealX 360, Forescout Technologies, Inc., Fortinet FortiNAC, Infoblox, Ivanti Neurons, LevelBlue USM, Lumen Managed Network Based Asset Discovery, NetSkope One, NetWatch.Ai, Palo Alto Networks - NGFW IoT Cloud Delivered Security Service, Solarwinds, Tanium Inc. Core Platform, Tenable Vulnerability Management, Zscaler Zero Trust Network Segmentation, 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: (Axonius Cybersecurity Asset Management, BlueVoyant Standard Vulnerability Scanning, Check Point - Infinity External Attack Surface Management, CrowdStrike, DarkTrace/Attack Surface Management, Divergent External Facing Asset Discovery, External-Facing Asset Discovery Services and Technology, ExtraHop RevealX 360, Fortinet FortiRECON, Google Mandiant Advantage Attack Surface Management, Invicti Enterprise, Ivanti Neurons for External Attack Surface Mgmt, Lumen Managed External Attack Surface Management, NetWatch.Ai, Palo Alto Networks - Cortex Xpanse, Recorded Future, Shodan Corporate, Tenable.ASM (Attack Surface Management), Tenable.IO - Vulnerability Management, Trend Micro Vision One Attack Surface Risk Management (ASRM), Wiz Advanced, No preference)

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

* What are the total assets under management?

*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 Technologies, Cloudflare CDN, F5 Distributed Cloud (XC), Fortinet FortiADC, Fortinet FortiWEB Cloud, 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: (Barracuda XDR Managed Endpoint Security, BlueAlly Managed XDR, BlueVoyant XDR Bundle (MDR+SIEM), Broadcom - Symantec Endpoint Security (SES), Carbon Black EDR by Broadcom, Check Point Harmony Endpoint, Cisco Secure Endpoint, CrowdStrike Falcon Complete for Endpoint Detection and Response, CyberArk Endpoint Privilege Manager (EPM), Cylance Endpoint Security, Darktrace/ENDPOINT, Dell MDR, Elastic, Fortinet FortiEDR, Halcyon Tech, Heimdal Unified Endpoint Detection & Response Solution, HighWire EDR Managed Service, Managed Endpoint Detection and Response (MEDR) - Qualys Multi Vector, Microsoft, Azure, MS Defender/SentinelOne, MixMode Endpoint Detection and Response, N-able Endpoint Detection and Response (EDR), Palo Alto Networks - Cortex XDR, Proofpoint - Identity Threat Detection and Response, Secureworks, Inc. (Secureworks) – XDR, SentinelOne - Singularity Complete, Vulnerability Management, and Vigilance, Sophos - Intercept X Advanced with XDR, Tanium Inc. Core Platform, ThreatSpike, Trellix TRX/MV6, Trend Micro Vision One Endpoint Security, 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 Security, Barracuda Email Protection, BlueVoyant Microsoft Content Delivery, Check Point - Harmony Email and Collaboration (HEC), Cisco Secure Email, Cloudflare Email Security, Darktrace/EMAIL, Forcepoint Email Security, Fortinet - FortiMail and FortiSandbox, Heimdal Advanced Email Security Solution, IRONSCALES, Lumen Managed Email Security, Microsoft Defender for Office 365, Mimecast Email Security - Cloud Gateway, Omnissa Workspace ONE, OpenText, Proofpoint - Email Security Protection (Proofpoint on Demand), Proofpoint - Tessian Adapative Email Security, Sophos Email Advance, Trellix ETP/Email Security, Trend Micro Vision One Email & Collaboration Security, XQ Msg, 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: (Arctic Wolf Managed Detection and Response, Avertium (MXDR Services for Existing Microsoft users), Barracuda XDR, BlueAlly Managed Security Operations Platform, BlueVoyant XDR Bundle (MDR + SIEM), Check Point Infinity MDR, Cisco XDR, Cloudflare Dashboard, Critical Start - Cyber Operations Risk and Response Platform, Crowdstrike Falcon for Security Operations Platform, Darktrace, Dell MDR, Dynatrace, Elastic, ExtraHop Networks RevealX, Forescout Technologies, Inc., Fortinet FortiAnalyzer, FortiSIEM, FortiSOC, Google Mandiant Google Security Operations (SecOps), Heimdal Security Operations Platform Solution, HighWire Networks SOC Managed Service, Hosted FortiSIEM, Infoblox, Legato Security (Legato) - Security Operations Center as a Services (SOCaaS), LevelBlue USM, Presidio Managed Detection and Response, MixMode Security Operations Platform (SOP), NetWatch.Ai, Palo Alto Networks - Cortex XSIAM, Proofpoint Identity Threat Detection and Response, ReliaQuest GreyMatter, RSM Defense, Secureworks, Inc. (Secureworks) - Taegis XDR, Semperis Directory Services Protector & Active Directory Forest Recovery, Snowflake - Security Operations Platform, Sophos MDR, Splunk - Security Operations Platform, Tanium - Secuirty Operations Platform, Tenable.ONE, ThreatBoard - Security Operations Platform (SOP) SaaS, Trellix XDR/Helix, Trend Micro Vision 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)

Identity Access Management (IAM)- Products or services responsible for providing centralized management for digital identities and control access to systems and data based on organizational policies.

*Are you requesting Identity Access Management (IAM) capabilities through this grant opportunity?

If Yes Requesting:
*Do you have a solution providing this capability deployed in your environment Y/N?

If Yes has Solution:

*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: Akamai Technologies, Avertium : IAM services for existing Microsoft Users, Beyond Identity, Cisco Identity Services Engine, Crowdstrike Identity Threat Detection and Response, CyberArk Identity, Fortinet FortiAUTHENTICATOR, IBM, Inc. Verify, Microsoft Entra ID, Okta Identity and Access Management (IAM) and Privileged Access Management (PAM) - Workforce Identity Cloud, Omnissa Workspace ONE, One Identity Safeguard and OneLogin, Proofpoint Identity Threat Detection and Response, RSA, SailPoint Identity Security, Stellar IT Solutions: SAML, OpenID, Oracle, No Preference)

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

* How many users will be protected by this solution?

*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)

Secure Access Service Edge (SASE)- Products or services responsible for combining networking and security services, and delivering both through a cloud-based framework that supports remote users, branch offices, and cloud applications.

*Are you requesting Secure Access Service Edge (SASE) through this grant opportunity?

If Yes Requesting:

*Do you have a solution providing this capability deployed in your environment

If Yes has Solution:

*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: (Akamai Technologies, Barracuda SecureEdge, Broadcom - Symantec Secure Access Service Edge, Check Point Harmony Connect (SASE), Cisco Secure Access, Cloudflare One, Dell Services: Zscaler with Zero Trust Services - Security, Software, Design and Configuration, Forcepoint, Fortinet FortiGate, FortiSASE, FortiClient, HighWire Networks SASE Managed Service, Island Enterprise Browser, Island Technologies, Lumen Managed SASE (Fortinet), Lumen Managed SASE (Versa), Microsoft Secure Access Service Edge (SASE), Netskope One, Palo Alto Networks Prisma Access, Skyhigh Security Service Edge, Versa Networks SDWAN and Verson Networks SSE, Zscaler Zero Trust Exchange, No Preference)

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

* How many users will be protected by this solution?

*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)

Vulnerability Assessment and Management (VAM) - Products or services responsible for enabling organizations to continuously scan their IT assets for security vulnerabilities, to evaluate the risks associated with these vulnerabilities, and to prioritize remediation efforts.

*Are you requesting Vulnerability Assessment and Management through this grant opportunity?

If Yes Requesting:

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

If Yes has Solution:

*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: (Armis VIPR Pro, Axonius Cybersecurity Asset Management, BlueAlly Managed Vulnerability Assessment and Management, Check Point Infinity Vulnerability Management, Cortex XSIAM, Critical Strike Vulnerability Management Services, CrowdStrike Falcon Spotlight, Dell MDR Vulnerability Management, Directory Services Protector & Active Directory Forest Recovery, Divergent Vulnerability Assessment and Management, Dynatrace, Forescout Technologies, Inc., Foresite Managed Autonomous Testing, FortifyData Enterprise, Fortinet FortiScanner Cloud, FortiClient EMS, Heimdal Advanced Vulnerability Management Solution, HighWire Networks Vulnerability Management Managed Service, IBM - Gaurdium Vulnerability Assessment, InsightVM, Invicti Enterprise, Ivanti Neurons for Patch Management, Nessus, Omnissa Workspace One, Palo Alto Networks Cortex XSIAM, Rapid7 InsightVM, Recorded Future, Ret Hat, Inc. Insights, SecPod Technologies, SanerNow, Secureworks, Inc. (Secureworks) – VDR, Semperis Directory Services Protector & Active Directory Forest Recovery, Tanium Vulnerability Assessment and Management, Tenable Vulnerability Management, ThreatBoard - Vulnerability Assessment and

Management (VAM) Saas, Trend Micro Vision One Attack Surface Risk Management (ASRM), Vulnerability Assessment and Management, Wiz Advanced, Zscaler Unified Vulnerability Management, No Preference)

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

* How many endpoints (Windows, Linux, MacOS) will be protected by this solution?

*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)

Data Security - Products or services responsible for protecting sensitive information from unauthorized access, loss, or exfiltration.

*Are you requesting Data Security through this grant opportunity?

If Yes Requesting:

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

If Yes has Solution:

*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: (Antivirus for Amazon S3 (AVS3), Assured Rubrik Data Security Solution, BigID for Data Security, Compliance, Privacy, and AI, Broadcom - Symantec DLP, Cisco User Protection Suite, Cohesity, Commvault Cloud, Powered by Metallic AI, Cribl Edge, Lake, Stream and Search, CrowdStrike Data Protection, Data Loss Prevention, Data Security Posture Management, ForcepointOne SSE, Fortinet FortiDLP, IBM Guardium, Island Enterprise Browser, Island Technologies, Stellar IT Solutions: Microsoft Purview, Informatica, NetSkope One, NVISIONx, OpenText, Palo Alto Networks Prisma SASE / Strata Data Loss Prevention / Cortex
Privacera, Proofpoint Adaptive Email DLP, Proofpoint Information Protection, Rubrik Security Cloud and Data Security Posture Management, Snowflake, Trellix DLP, Varonis Data Security Platform, Wiz Advanced, Zscaler Data Protection, No Preference)

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

* How many users will be protected by this solution?

*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).

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? (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