THE GOVERNING BOARD OF THE
ST. JOHNS RIVER WATER MANAGEMENT
DISTRICT

REQUEST FOR INFORMATION 38413 — WIDE AREA NETWORK AND INTERNET, MANAGED NETWORK SECURITY SERVICES, AND LONG-DISTANCE SERVICES

The Governing Board of the St. Johns River Water Management District (the "District") requests that interested parties respond to the solicitation below by 2:00 p.m., December 28, 2022. Further information is available through DemandStar at *Demandstar.com* [(800) 711-1712], Vendor Registry at *Vendorregistry.com*, or the District's website at *sjrwmd.com*. Solicitation packages may be obtained from DemandStar, Vendor Registry, or the District by calling or emailing Kendall Matott, Sr. Procurement Specialist, at (386) 312-2324 or kmatott@sjrwmd.com. Responses will be opened in the Procurement Conference Room, Administration Building, Palatka Headquarters, 4049 Reid Street, Palatka, Florida 32177-2571.

The purpose of this solicitation request is to gather information on available options to provide the District with a wide area network, internet, managed network security services, and long-distance services. This is for information purposes only; therefore, the District is under no obligation to purchase any services or products based on the information submitted. The information provided to the District may be used to develop a statement of work for a subsequent or future procurement action.

The District's Evaluation Committee will meet at District headquarters at 4049 Reid Street, Palatka, Florida 32177-2571, to evaluate and rank Submittals as follows:

- 10:00 a.m. and 2:00 p.m., on January 11, 2023, to
  - Discuss the responses and information received
  - Decide if oral presentations (by some or all Respondents) are necessary to assist in facilitating the evaluation process to determine the District's future needs and requirements for these services
- 9:00 a.m., January 17-18, 2023, to
  - Hold oral presentations of some or all Respondents – oral presentations may be provided in person, via telephone or online, or a combination of these options

Americans With Disabilities Act (ADA)

The District does not discriminate on the basis of disability in its services, programs, or activities. Special accommodations for disabilities may be requested through Kendall Matott, or by calling (800) 955-8771 (TTY), at least five business days before the date needed.

RFI 38413 — WIDE AREA NETWORK AND INTERNET, MANAGED NETWORK SECURITY SERVICES, AND LONG-DISTANCE SERVICES

I. INTRODUCTION

The St. Johns River Water Management District (District) is considering replacement of our voice, data, and network security services service provider. We are interested in learning of any new developments or technologies to the industry or issues based on current events that would impact our decision. The future project would entail the Successful Respondent to provide, install, manage, and support the District's Wide Area Network (WAN) and internet connectivity, managed firewall and network security services, and voice services.

The District has ten locations: Palatka Headquarters with approximately 500 employees; Apopka, Palm Bay, and Jacksonville service centers with approximately 30 – 70 employees each; Umatilla and Mt. Dora field offices with ~15 employees each; and the Hawthorne, Bayard, Geneva, and Seville field offices with three employees each.

Respondents are welcome to submit information on one, or a combination, of the services requested. Respondents are also encouraged to submit on alternative technologies to accomplish these services. The District may utilize this information in preparing a follow-on procurement action for such services.

II. OBJECTIVES

The objective of this Request for Information is to gather information on

- WAN and internet connectivity; managed firewall and network security services; and voice services, including long distance and international calling.
- Training for all systems and hardware.
- Technical and billing support, escalation process and Service Level Agreement (SLA).
- Hardware availability and delivery lead times.
- Connectivity to Amazon Web Services (AWS), Azure, and Oracle Cloud Infrastructure (OCI) cloud-based services.

III. DETAILS

WAN and Internet Connectivity

Background

The District's ten locations are connected via VeloCloud SD-WAN routers on fiber links of various sizes and providers. All sites have their own FortiGate firewalls and connect directly to the Internet as well as the WAN. Each site also has a redundant link, typically cellular via Cradlepoint routers. The District Headquarters (DHQ) has two 500Mbps fiber links setup as geographic and vendor diverse circuits. The circuits are load-balanced in an active/active pair to allow full use of all available bandwidth as well as dynamic redundancy should a link be cut. The Apopka Service Center (ASC) will soon house our backup Data Center and SAN and has a 200Mbps fiber circuit with a 5G Cradlepoint redundant link setup as active/standby. Palm Bay also has a 200Mbps circuit as it currently houses our backup Data Center and SAN. This site has an LTE Cradlepoint for its active/passive backup link. All other locations, no matter the size, have a 100Mbps fiber circuit with an LTE Cradlepoint for active/passive backup. All these links are dedicated fiber into each facility. The District is interested in maintaining this current mesh topology via SD-WAN, but is open to new technologies or strategies to improve our network's performance and security.

Preferences

- All sites bandwidth should remain the same or be increased.
- Palatka HQ will maintain two fiber links for redundancy and resiliency, with both physical and vendor diversity between the two circuits. These links shall be configured for load balancing.
- All sites must have a cost-effective redundant backup link that is adequate to, on a basic level, support staff and operations when the primary link is down.
- All sites shall be able to route directly to each other in a mesh topology.
- All sites shall maintain a local internet link; internet traffic shall not route through Palatka HQ.
- The District prefers VeloCloud customer premises equipment (CPE) SD-WAN hardware. Updated models are encouraged and new manufacturer hardware solutions will be considered.
- All CPE hardware shall have SNMP, SYSLOG, and NETFLOW configured to point to District NMS server.
- All CPE hardware will be contractor-managed with limited District co-management and visibility. The District prefers that the vendor provide, own, and support all hardware.
- All equipment should be new and should have specs capable of supporting one gig of bandwidth at each site so the District has the option of expanding services in the future.
- Respondent must provide anticipated lead times for proposed equipment for through FY23-24.
- Respondent must confirm capability to monitor all links, circuits, and routers provided 24/7/365 and capability to provide immediate and useful alerts and responses when trouble occurs.
- Respondent shall describe that the means to tune alerts and notifications to reduce alerting on known issues or false positives. Alerting shall support more than one individual.
- The District must be provided visibility into the non-proprietary configuration of the CPEs, that is the District doesn't require privileged access, passwords, encryption keys or vendor internal IPs, but will need the ability to see basic configurations like interfaces, routing, and VLANs.
- Respondent shall confirm that it has the capability to move the District's Class C subnet to its network for advertisement and provide District-accessible /28 network for each location for configuration of firewalls (FW) and CPE.
- The District is currently investigating cloud based options for our data and services. We would like to understand the Respondent's capabilities in integrating with Azure, OCI, and AWS cloud infrastructures and recommendations on how to best prepare for and connect our networking infrastructure to those and other cloud-based services.

Managed Firewall and Security Services

Background

The District currently utilizes TPx for managed security provider services and Fortigate firewalls to protect its network at the edge. TPx provides 24/7/365 managed security, monitoring, tracking and notification. TPx also provides monthly vulnerability scanning of DMZ systems with PDF and CSV reports.

The Fortigate firewalls are owned by the District and co-managed by TPx and the District, meaning District staff have the same direct access to manage, monitor, and configure the FWs as TPx. In addition to standard traffic filtering, the firewalls perform all of the District's name address translation (NAT). The FWs also performs content, Antivirus, Anti-Botnet, and geo-IP filtering along with intrusion detection and prevention (IDP). The FWs are capable of deep packet inspection- secure socket layer (DPI-SSL) but

that is not currently configured and something we have interest in deploying. The Fortigate FWs also terminate the District's SSL virtual private network (VPN), both at Palatka HQ and at Apopka.

Preferences

- Respondent shall state its ability to provide similar or better capacity FWs with a high availability (HA) pair at Palatka HQ. The FWs shall have 10G interfaces for LAN uplinks and meet or exceed specs for current model, Fortigate 300E. (Fortigate preferred, but other solutions will be considered).
- Respondent shall state its ability to provide Firewalls for all remote offices at specs that match or exceed current hardware; Fortigate 100E, 80E, 60E. (Fortigate preferred, but other solutions will be considered).
- Respondent shall state its ability to support all current and proposed FW features.
- All FWs shall be of a single vendor and managed by a single management console.
- The District must be provided co-manageability of FWs.
- The District is open to utilizing a separate device to terminate the VPN.
- The District is interested in other methods of remote access, including Microsoft DirectAccess.
- FWs must be configured for SNMP, email notifications, and SYSLOG to District network management service (NMS) servers, which are currently Solarwinds Orion and FortiAnalyzer.
- Respondent shall state its ability to provide 24/7/365 management and monitoring of network traffic for security incidents, conduct security analysis, provide useful and timely notifications, and advice on resolution steps.
- Respondent shall describe that the means to tune alerts and security notifications to reduce alerting on known issues or false positives. Alerting shall support more than one individual.
- Respondent must confirm ability to provide monthly Vulnerability Scans that can provide detailed reports in both PDF and CSV/Excel format (for import into automated tracking system) or Direct access to Vulnerability Scanning Portal that provides the ability to assign vulnerabilities to staff for resolution, track progress, and mark vulnerabilities and patched or accepted.

Voice Services

Background

The District currently utilizes 2 Session Initiation Protocol (SIP) trunks with 42 call paths each. One SIP trunk is at Palatka HQ and the other is at our Palm Bay Service Center. They are completely redundant and have all DIDs advertised on both. 911 is provided thru the SIP trunks. There are various analog lines across the District for a host of reasons, including alarms, elevators, and modems. We currently use Mitel (Legacy Shoretel) as our PBX, however, we are in the process of investigating cloud-based phone system options. Replacing the PBX with a cloud-based phone system will be an independent project, separate from a WAN, Internet, MSS, and Voice Services project, however, we welcome input and information from respondents. All analog lines are provided by either SUNCOM or CenturyLink and will not be modified or covered under any future project.

Respondents should provide information on the following:

Preferences

- Responded should confirm ability to provide SIP trunks. Other solutions will be considered, but SIP is preferred.
- For SIP solutions, Respondent should provide a demo SIP solution during its oral presentation and information as to whether the District can have an opportunity to use such services for a limited time for evaluation purposes.

- All solutions must integrate seamlessly with the District's current Mitel Connect system.
- Respondent shall confirm that it provides minutes-based cost plans or unlimited minute plans, and for which locations. Plans should include all types of domestic long distance, including interstate, intrastate, interlata and intralata.
- Respondent shall provide plans for international calling Plans; however, the District makes limited international calls.
- Respondent shall describe how 911 forwarding over SIP is provisioned including whether subcontractors are utilized.
- Respondent should state its ability to port all current phone numbers and DIDs to the new solution, including Toll Free and any analog lines.

IV. SUBMITTAL REQUIREMENTS

In order to assist with the District's review process, the product information package shall be prepared utilizing the following format. Each of the required sections is to begin a new page and be separately tabbed or identified. One original and four copies shall be delivered.

Respondents are encouraged to include as much pertinent data and information under each section as necessary to ensure proper evaluation of the information.

The format is as follows:

Section 1. **Title Page** — Show the Request for Information subject, the name of your company, address, telephone number, fax number, email address, name of contact person, and the date.

Section 2. **Table of Contents** — Clearly identify material by section and page number.

Section 3. **Letter of Transmittal** — Limit to two printed pages. Briefly describe your company's understanding of the purpose of this Request for Information.

Section 4. **Marketing Documents** — Include all information requested. Provide brochures, promotional materials, and/or demonstration CD or pin/thumb/jump drive.

V. RESPONSES

Responses must be submitted in an electronic format (i.e., jump or thumb drive).

The District recommends that Respondents confirm their Submittal will open correctly on a non-company owned computer. Any submittal received by the District that does not open on a District-owned computer is subject to rejection as a defective response. **Please do NOT password protect your electronic files.**

All electronically submitted files shall be saved to a single pin/thumb/jump drive. The pin/thumb/jump drive MUST be placed in a sealed envelope pursuant to the instructions under Item 3 for sealed responses – **DO NOT SUBMIT YOUR RESPONSE BY EMAIL — THIS WILL RESULT IN THE SUBMITTAL BEING REJECTED AS NON-RESPONSIVE.**

VI. INQUIRIES

Further questions regarding this Request for Information shall be directed to Kendall Matott, Sr. Procurement Specialist, (386) 312-2324, kmatott@sjrwmd.com, or by writing the St. Johns River Water Management District, 4049 Reid Street, Palatka, Florida 32177.