Jackson County Library Distrixt RFP NUMBER: #2025-03
Questions & Answers, July 10 2025

	QUESTIONS	ANSWERS
	Overall Notes for Responding to the RFP	
1	RFP respondents are required to read and respond to all elements of the RFP, documenting any exceptions to specifications or contract or other terms **within** their RFP response. Following selection of the winnding bidder, contractual exception negotiations can be engaged.	
2	Respondents are directed to clearly review and understand Page 4 of the RFP, Item 2.1: Prospective service providers are not required to complete all of the Cybersecurity Pilot Program registration requirements prior to bidding, however, if their bids are selected, the winning service providers must register with USAC and SAM.gov by August 1st , so the District can complete the Cybersecurity Pilot Program applicant filing (Form 471).	
	Submitted Questions:	
1	When is the RFP submission due?	The RFP closes on July 20, 2025, 3:00 pm PST
2	Could you please confirm if the final proposals submitted should align with the quantities listed in the RFP?	Yes, they should
3	In terms of the total 300 licenses needed for endpoint what is the split between servers and devices?	224 Workstations 9 Servers
4a	How many servers do you have?	9 Servers
4b	What is the total # of On-Prem Servers?	
5a	Number of linux, windows, macOS Endpoint for laptops, desktops & server devices by type (excluding Chromebooks, iPads and android tablets) ?	224 Windows Laptops/Desktops, 7 Windows Servers, 2 Linux Servers
5b	What is the total # of Endpoints (laptops, desktops, servers + OS types)?	
6	What is the total # of IaaS/Cloud Servers (AWS, Azure, GCP)?	1 - Entra/Intune
7a	What is the total # of Users (employees generating network traffic, have access to a computer and corporate apps)?	We have ~224 users
7b	The RFP says up to 400 data sources, is that how many users we should assume?	

Jackson County Library Distrixt RFP NUMBER: #2025-03
Questions & Answers, July 10 2025

	QUESTIONS	ANSWERS
8	What is the total # of Cloud Monitoring Licenses with license level (O365, Google Workspace, Box, Salesforce)?	220 Microsoft 365 A3 for faculty (new licenses)
9	Are your endpoints primarily on-premises, remote, or hybrid?	On-Premises
10	How many IP addresses to scan?	Internal = 1,048,576 Our vlans are 10.x.x.x with a 16 bit subnet mask.
11	What is the current connection type between the Firewall and the Core Switch at each location (1Gb copper, 10Gb fiber, etc)?	5 GB at 14 to Main and 5 GB at main to firewall, 10 GB out from Firewall
12	What is the current Firewall vendor, model number(s) and software feature set?	XGS3300 (SFOS 21.0.1 MR-1-Build277) X330048RFY77H44 with intrusion detection and content filtering features.
13	Can you provide a basic summary of their network device types (routers, switches, firewalls, UTMs, VPNs, Active Directory servers, LDAPs, DHCP, DNS, syslog-capable systems, etc) for log retrieval?	2 firewalls – 1 is set for failover 27 Switches 2 Active Directory Servers with DNS Sophos Firewalls, Juniper Switches, Aruba Wifi, on prem Windows 2016 servers.
14	What is the total # of Locations with direct internet access & # of Firewalls (internet facing) per location? (please note if any locations have HA Pair configuration)	1 location and 2 firewalls with one set as failover Our internet provider delivers our branches vlan trunks directly to our Medford IDF firewalls, which then apply filtration and NAT to outgoing traffic. Layer 3 switches are the only hardware at branches.
15	Do you have virtualization hosting capabilities, e.g. VMWare, for MDR on-premises components (Log Collector, Honeypot, Orchestrator, Vulnerability Scanner VMs)?	No, we do not.
16	Do you require SOAR (Security Orchestration Automated Response) capabilities?	Not required, but considered a benefit.
17	Do you require proactive Threat Hunting by SOC Analysts?	Not required, but considered a benefit.

Jackson County Library Distrixt RFP NUMBER: #2025-03
Questions & Answers, July 10 2025

	QUESTIONS	ANSWERS
18	Do you require internal Vulnerability Scans to assess and prioritize critical vulnerabilities for remediation of non-endpoint systems (IoT devices, network infrastructure, network appliances)?	Not required, but considered a benefit.
19a	Do you need to retain MDR security data for longer than 60 days (up to 365 days)?	Up to 365 days
19b	Do they (endpoints) need to retain EDR security data for longer than 30 days (ex., 90, 180, 365 days)?	
20	Do you need monthly or quarterly security reviews & briefings of their network's security posture?	Monthly
21	Do they need dedicated security team where SOC analyst will have good knowledge of customer's network environment?	Yes
22	What level of visibility do you need into endpoint activity (e.g., file access, process execution)?	Process execution at a minimum
23	Are you interested in deploying Deception Technology (Honeypots) to asses attacker behavior & intent ?	We are interested, yes.
24a	Do you need MDR to monitor cloud-based SaaS services ?	Yes - Microsoft 365 and Microsoft Entra/Intune
24b	Do you need MDR to monitor cloud-based SaaS services?	
24c	Please list cloud-based services ?	
24d	What is your current MFA vendor and solution?	
25	Do you need network sensors to monitor network traffic between endpoints and network infrastructure?	We don't need it, however network intrusion monitoring across the switching fabric is something that we are interested in.
26	Characterize expected traffic (network segment count, volume GB/TB, rate Gbps)?	Approximately 100 vlans routed through Sophos firewalls. Peak WAN traffic in the last 10 days hit 320 MB per second.
27	Can you host hardware or virtualized network sensors at these locations?	No. We currently do not maintain a virtualization cluster.

Jackson County Library Distrixt RFP NUMBER: #2025-03
Questions & Answers, July 10 2025

	QUESTIONS	ANSWERS
28	Please describe the current distribution of duties between JCLD and Huntress. (i.e., Is JCLD using Huntress EDR unassisted? Is Huntress managing JCLD's Defender for Endpoint deployment? Some combination of both?)	Huntress provides its EDR which controls Defender for Endpoint via policy. Outside of critical response escalations to EDR signals, Huntress does not actively manage our environment.
29	What License level is JCLD currently utilizing with Defender for Endpoint?	Defender for Endpoint plan 1 (bundled with Microsoft 365 A3 for Fac)
30	Prior to engagement with Huntress, was JCLD already leveraging Defender for Endpoint?	No. Prior to modern EDR, we used Avast Anti-Virus.
31	Outside of Huntress, does JCLD leverage additional Managed Service Providers for security services? If so, who is the provider and please describe the level of services	Beyond what comes with Microsoft 365 A3, Huntress EDR is our only security service/product.

END OF QUESTIONS