Department of Procurement
MONTGOMERY COUNTY PUBLIC SCHOOLS
45 W. Gude Drive, Suite 3100
Rockville, Maryland 20850

September 25, 2025

NOTICE TO RESPONDENTS

The following are questions and responses regarding
MO26-47002-C2-Firewalls - Form_470_Application_260001094

Question 1: **Does the user count at each school vary significantly, or are they all roughly the same size?**

Answer 1: The user count at each school varies significantly.

Question 2: **Section 4.1 – Main Firewall – Technical Requirements**

a. Could you provide the maximum throughput and concurrent connection count for your main firewall, ideally with and without all security services enabled?
b. Any specific IPSEC VPN throughput requirement?
c. Does your current firewall have reporting capabilities for a concurrent session count per-site? If so, can you share that data?
d. How many **VDCs (Virtual Device Contexts)** are currently deployed in the existing Cisco Nexus 7009 switches?

Answer 2: **Section 4.1 – Main Firewall – Technical Requirements**

a. The maximum throughput as advertised is 100Gps and 79.9 GPS with decryption. We peak at around 6 million sessions per second
b. N/A
c. No
d. 3

Question 3: **Section 4 – 4.3 Experience & References:**

a. Is submitting experience/references with MCPS and in education/K-12 environments is a mandatory requirement?
b. Can firm submit experience with other sectors like SLED [healthcare and other] or FED other than MCPS and education/K-12 environments?
c. Can we submit experience/references from our proposed subcontractor?
d. Are commercial experience/reference permitted?
e. Can Case studies or examples be other than from regional school districts?

Answer 3: **Section 4 – 4.3 Experience & References:**

a. no
b. yes
c. yes
d. yes
e. yes

Question 4: **Section 5. Pricing Structure:**
Will the agency be adding pricing worksheet or firm are required to create their own?

Answer 4: Respondents are required to create their own pricing structure.

Question 5: **Attachment A MCPS General Contract Articles**
ARTICLE 22. INDEMNIFICATION AND LIABILITY, Point D states *"The Contractor expressly understands and agrees that any performance bond or insurance protection 16 required by the Contract, or othe1wise provided by the Contractor, shall in no way limit its responsibility under the Contract to defend, indemnify, and hold harmless MCPS"*

a. Could the agency clarify if there any performance bond or insurance protection applicable to this solicitation? if yes please provide details.
b. ARTICLE 23. INSURANCE: Are firm required to provide any proof of insurance with the bid?
c. Attachment A: ARTICLE 23. INSURANCE: Is it a post-award requirement?

Answer 5: **Attachment A MCPS General Contract Articles**

a. There are no performance bond or insurance protection applicable to this solicitation.
b. This is a post-award requirement.
c. This is a post-award requirement.

Question 6: **Solution Sizing & Performance**

a. To ensure our solution is accurately sized for both current and future needs, can you provide the current and projected future Internet and MPLS bandwidth, including peak utilization, for your main data center?
b. What are the current and projected total and peak daily bandwidth, along with the peak number of concurrent sessions and new sessions per second, for a typical high school and the primary data center?
c. What are the current average and peak logs per second (LPS)across each of your firewalls?
d. What is the current and anticipated amount of SSL/TLS encrypted traffic that will require decryption and inspection?

Answer 6: **Solution Sizing & Performance**

a. 40G daily, 70G peak, 200G projected
b. 3G daily, 8G peak, 10G projected
c. 125K per second/per day peak
d. All outbound traffic will require decryption and inspection

Question 7: **Security & Compliance Strategy**

a. The RFP mentions a desire for advanced security. What is your current strategy for handling unknown threats and zero-day attacks, and what are your primary objectives for improving this capability?
b. Could you describe your current or desired approach for segmenting traffic within your network, especially from a compliance perspective? We would like to understand whether that approach varies at the data centers, high schools, and other locations.
c. What is your current strategy for enforcing granular access controls based on identity, role, and security posture?

Answer 7: **Security & Compliance Strategy**

a. MCPS relies on the vendor provided tools for threat detection and zero-day attacks. Enhanced reporting and ease of producing actionable intelligence.
b. Currently, traffic segmentation is only done at the subnet level where each security zone is virtually segmented by VLAN. We would like to expand on this architecture allowing for enhanced segmentation at the user and application levels
c. Access controls based on identity for categorical web access are via generalized groups (either Entra or Google). Wireless subnets are segmented via VLANs after authenticating with their user credentials (e.g., staff, student, domain-joined device).

Question 8: **Deployment & Integration**

a. The RFP asks for our deployment options. To ensure our proposal is tailored to your needs, please clarify if you are looking for a description of our recommended deployment methods (e.g., on-premise appliances, cloud-delivered services, or a hybrid model), or if you have a specific deployment architecture in mind that you would like us to respond to.
b. What are your key goals and desired approach for real-time traffic analytics and automated reporting?
c. What existing monitoring tools do you currently use that would need to be integrated with a new solution?

Answer 8: **Deployment & Integration**

a. MCPS is seeking vendor recommended solutions and vendors need to respond with what they can do.
b. Realtime reporting should provide summary data (e.g., current throughput, recent threats.). Automated reporting is helpful, but depends largely on the technology (threats are mostly users searching YouTube for lyrics, counters, etc.).
c. Ingestion or correlation of web logs would be helpful for an initial implementation, but it depends on whether we would continue to use our current deployment or switch to a proposed web content filtering solution.

Question 9: **Cloud-Native Secure Remote Access Connection**

a. To ensure our solution is sized appropriately for your needs can you provide:
   - The total number of users and contractors who require remote access.
   - Average and peak number of concurrent connections.
   - Average and peak daily bandwidth usage per remote user in Mbps
b. With your current VPN solution, are you ingesting logs into your SIEM?
   - If so, can you provide an estimate of the volume in GB per day that the VPN generates? This information is critical for planning the log collection and analytics portion of the new solution.

Answer 9: **Cloud-Native Secure Remote Access Connection**

a. To ensure our solution is sized appropriately for your needs can you provide:
   - About 1,300 unique users out of a group of 34,000
   - Peak around 800 daily
   - Information not available
b. With your current VPN solution, are you ingesting logs into your SIEM?
   - Yes, both authentication and user traffic is logged in the FortiAnalyzer.

Question 10: Strategic Vision & Hybrid Topology

a. The RFP references your existing MPLS connectivity and need for remote site modernization. Are you open to a **hybrid network topology** that combines a dedicated data center switching fabric with a separate, cloud-delivered SD-WAN solution that manages the WAN traffic across for your remote sites? For example, your central IT team could create a consistent policy in a single interface that ensures CIPA-compliant content filtering is applied to all student traffic from your 211 schools, regardless of the underlying internet provider. This approach would allow you to optimize the data center for performance while gaining simplified, centralized management and visibility for your entire distributed network, a key benefit for large school systems like MCPS.

b. What is the overall objective and strategic vision you hope to achieve with an **SD-WAN solution** in your environment? Please describe with sufficient detail.

Answer 10: Strategic Vision & Hybrid Topology

a. Yes. MCPS is seeking vendor recommended solutions and vendors need to respond with what they can do.

b. SD-WAN was not specifically mentioned in MO26-47002-C2-Firewalls _260001094 RFP. MCPS is seeking vendor recommended solutions and vendors need to respond with what they can do.

Question 11: Network Architecture & Sizing

a. To ensure proper sizing and deployment, please provide details on your WAN connections, including the specific ISP carriers at each remote location, whether bandwidth varies by site type, and the current bandwidth for your disaster recovery sites.

b. For each nondata center site type, please describe your current segmentation approach and whether the MPLS network is considered a trusted segment. This will help us understand your security posture and design for encrypted transport.

c. What is the current routing protocol being used for your WAN and remote sites (e.g., BGP, OSPF)?

d. To ensure we meet your availability requirements, please specify which non-data center site types require high-availability and the count for each.

e. How do you currently measure end-user experience for students, educators, and administrators? What specific applications or services (e.g., online learning platforms, collaboration tools) are most critical, and what is your process for responding to service degradation?

f. What cloud services providers (CSPs)do you currently and project to use in the future? If you're currently using a CSP, please indicate which region or zone and whether any direct connect (e.g. ExpressRoute or Direct Connect) is utilized or planned in the future.

g. Our solution is designed for a phased migration. How would you like to begin with an initial deployment at a small number of remote sites before a full-scale rollout?

h. What is the expected number of remote network sites to be managed by the SD-WAN solution?

Answer 11: **Network Architecture & Sizing**

a. 1G MPLS @ ES : 10G MPLS @ MS : 10G MPLS & 1G @ HS respectively. DR = 100G MPLS & 30G ISP
b. Not segmented and yes, it is a trusted network
c. BGP
d. None
e. MCPS does not measure end-user experience. Our critical applications are Google Workspace apps, Canvas, Synergy, Oracle Hub.
f. Azure and Synergy (via AWS)
g. Yes, a small pilot to begin
h. 250

Question 12: **Chromebook Sizing & Usage -** To ensure we can properly size our solution, can you provide the total number of Chromebooks in your environment, the estimated number used off-network daily or weekly, and the average daily data volume they generate in gigabytes?

Answer 12: **Chromebook Sizing & Usage -** 189K active Chromebooks, 47K off-network daily, and 15TB daily data volume.

Question 13: **Chromebook Security & Management**

a. To fully support your Chromebook environment, what are the current security requirements and policies for these devices when they are used off-network? What are your key concerns or goals related to traffic management in this scenario?
b. Do you experience any performance or latency issues with your current security solution for off-network Chromebooks?
c. How important is it for you to have a single, unified platform for DNS security that provides consistent protection for all devices, whether they are on-network or off-network?
d. The RFP mentions advanced URL filtering and CIPA compliance. How important is it for you to have a single, unified platform for DNS security and URL filtering that provides consistent protection for all devices, whether they are on-network or off-network?
e. How critical is it for your school district to have a unified logging and analytics platform to monitor security events and DNS queries from all devices, both on and off-premise?

Answer 13: **Chromebook Security & Management**

a. Devices have the same technical policies applied regardless of location, and users are expected to follow our acceptable use policies. The primary security concern for Chromebooks is web content filtering. The primary general concerns are regulatory compliance (e.g., federal regulations regarding explicit and harmful content) and configuration consistency (e.g., the same policy applies to an individual user/device regardless of location)
b. Our current platform has minimal performance issues, although latency differs between the two vendor data center points-of-presence by 15ms or so (US-East and US-Central). Devices are not specifically assigned access through either data center.
c. Specifically for off-network, this would be a new feature. MCPS is seeking vendor recommended solutions and vendors need to respond with what they can do.

d. Yes, it is important to have a unified platform for DNS security and URL filtering.
e. Extremely important.

Question 14: Current Security Operations & Challenges

a. What is your current SIEM platform, and what are its biggest limitations? We are particularly interested in understanding the most common challenges your Security Operations Center (SOC)team faces on a day-to-day basis, as well as any existing gaps in visibility you are looking to improve.
b. To what extent is your current SIEM integrated with your security devices, Chromebooks, and third-party systems? What are your key objectives for unifying these data sources in a new solution?

Answer 14: Current Security Operations & Challenges

a. FortiAnalyzer. One of our biggest challenges is log collection and insertion latency at peak times. Reporting is often inaccurate or incomplete.
b. The current SIEM is not integrated with all the security solutions. Implement a solution that allows engineers to correlate logs from a single platform.

Question 15: Future Security Platform & Strategic Goals

a. What is the required amount of time that you need to hold logs in hot, warm, and cold storage tiers for compliance and investigations?
b. How much effort is spent by your team managing and manually correlating data from multiple security consoles? What value would a unified security operations platform bring to your security team by automating these tasks?
c. The RFP mentions addressing critical gaps identified in internal and OLA audits. How important is it for a new security platform to simplify compliance reporting and provide a centralized view of your security posture across the district?
d. What are the most time-consuming aspects of threat hunting and forensic investigations in your current environment, and how important is it to automate these processes?
e. To help us better understand your needs, can you provide a few use cases or scenarios that you would like to be able to address with a new security platform?

Answer 15: Future Security Platform & Strategic Goals

a. Minimum of 90 days.
b. A lot of effort is spent managing and manually correlating data. A high value.
c. Very Important .
d. Log searches and manual correlations.
e. Search a user's activity and identify attempts to bypass content filtering.

Question 16: 3.1 Core Firewall Services

a. Do the current Security Capabilities account for Data Loss Prevention (DLP) policy enforcement to proactively detect and prevent attempts to transfer sensitive data to unauthorized destinations in real-time?

b. Does MCPS have other solutions in place for URL/content filtering today that you're planning to offload to physical firewalls for full management or is MCPS planning to utilize physical firewalls only as a supplemental solution?

Answer 16: **3.1 Core Firewall Services**

a. No
b. MCPS is seeking vendor recommended solutions and vendors need to respond with what they can do.

Question 17: **3.2. School Site Firewalls or Cloud Services - Does the current Scope of Service account for a cloud-managed SD-WAN solution for all high school, middle school, and elementary school sites? If yes, how many sites should be included as part of a proposed SD-WAN solution?**

Answer 17: MCPS is seeking vendor recommended solutions and vendors need to respond with what they can do for all high schools only.

Question 18: **Section 1: The introduction indicates learning programs across 211 schools while the FCC Form 470 identifies 253 eligible entities. Does the 253 count reflect all entities actively participating in this procurement and, if so, is there any clarifying information that would help identify the full scope?**

Answer 18: MCPS has 253 entities actively participating in this procurement. All quantities are approximate and subject to change. The specification, quantity, capacity, locations, and count of services will vary over time due to fluctuations in the School District's needs. Printable list of schools and office sites can be found here https://ww2.montgomeryschoolsmd.org/schools/index.aspx

Question 19: **Section 2: Can you clarify whether MCPS prefers cloud-delivered firewall services or on-premises appliances for the main firewall solution?**

Answer 19: We have no preference, we are doing evaluations to help determine our path forward.

Question 20: **Section 2: Is there a preferred vendor list or any restrictions on product selection?**

Answer 20: No

Question 21: **Section 2: Will MCPS provide network topology diagrams or current infrastructure details for planning?**

Answer 21: Yes, at the time of award.

Question 22: **Section 2: Are there any legacy systems that must be supported during the transition?**

Answer 22: Yes

Question 23: **Section 2: What is the expected throughput and concurrent session capacity required for each firewall?**

Answer 23: At least 100 GPS of throughput and at least 8 million concurrent sessions.

Question 24: **Section 2: Are there specific performance benchmarks or latency thresholds for cloud-based ZTNA and VPN services?**
Answer 24: Yes, any cloud-based solution must deliver consistent low latency access; as a baseline, we expect below 50ms of additional latency.

Question 25: **Section 2: Will MCPS provide test environments or require a pilot deployment before full rollout?**
Answer 25: MCPS will require a full Proof of Concept (POC).

Question 26: **Section 4.1: Are there any existing integrations (e.g., SIEM, NAC, Azure AD) that must be preserved or migrated?**
Answer 26: SIEM and Azure AD

Question 27: **Section 4.1: What is the expected timeline for deployment across all 30 high school sites?**
Answer 27: The effective date of the awarded contract will be July 1, 2026. Delivery, setup and start of work will occur after the effective date of the awarded contract.

Question 28: **Section 4.1: Are there any reporting formats or tools MCPS prefers for compliance and audit logs?**
Answer 28: MCPS is seeking vendor recommended solutions and vendors need to respond with what they can do.

Question 29: **Section 4.2: What specific NIST, CISA, or K–12 cybersecurity frameworks must the solution comply with?**
Answer 29: NIST 800, NIST CFS

Question 30: **Section 4.2: If a vendor does not have direct MCPS experience and/or in education/K-12 environments, and/or regional school district case studies/examples, but has relevant experience, are they allowed to bid?**
Answer 30: Yes

Question 31: **Section 4.3: Are there any restrictions on remote access policies for contractors vs. internal staff?**
Answer 31: Yes

Question 32: **Section 4.3: Are there any SLAs or response time expectations for support and maintenance?**
Answer 32: Yes, MCPS requires real-time support for emergencies and prompt support for all other requests.

Question 33: **Section 5: What level of training and documentation is expected for MCPS IT staff?**
Answer 33: High level of training and documentation must be comprehensive.

Question 34: **Section 5: Will MCPS require on-site support or is remote support sufficient?**
Answer 34: Remote support is sufficient, provided there is a mechanism to access advanced support directly.

Question 35: **Section 2: On "Modern Instructional Delivery": "You state in Section 2 that your legacy systems 'lack the capability needed to fully support modern instructional delivery.' Could you detail the vision for what that looks like? What are the key applications, tools, and user experiences you need to enable?"**
Answer 35: MCPS is seeking vendor recommended solutions and vendors need to respond with what they can do. It is the vendor's responsibility to demonstrate that this solution is compatible with the MCPS infrastructure.

Question 36: **Section 2: On Performance & Scalability: "You mention performance and scalability as key drivers for this replacement. What specific bottlenecks with your current FortiGate appliances are causing the most friction for students, teachers, and your IT staQ today?"**
Answer 36: Daemon crashes, instability in configuration syncing, IPS engine failures are just a few of the primary causes of "friction."

Question 37: **Section 2: On Security Beyond the Firewall: "As a K-12 district, protecting student data is paramount. Beyond basic firewalling, how high a priority is securing against data loss (DLP) to protect PII data?" should we ask if DLP is part of this project or a separate project?**
Answer 37: MCPS is seeking vendor recommended solutions and vendors need to respond with what they can do for all high schools only.

Question 38: **Section 2: Mentions requiring flexible connectivity options. Can you clarify what options you are looking at?**
Answer 38: MCPS is seeking vendor recommended solutions and vendors need to respond with what they can do.

Question 39: **Section 3.1: How many Core firewalls are there? What are those Core Firewalls by OEM? What functions do these Core firewalls do? What is the bandwidth capabilities of these Core firewalls? How many users do those Core firewalls support access for? What is the projected growth of the core firewalls in terms of bandwidth and user growth?**
Answer 39: **Section 3.1**

a. 3
b. Fortinet 7060E 8
c. NGFW, IPS, NAT
d. 100G
e. 100Gps and 79.9 GPS with decryption
f. 185,000
g. Unknown ATM

Question 40: **Section 3.2: How many users need access at each school location? Are these users faculty and staQ? What is the anticipated future growth of users over next 5+ years? We should also ask if this includes student traQic also**

Answer 40: **Section 3.2**

a. This varies between school enrollment. Data available on the website - https://ww2.montgomeryschoolsmd.org/departments/sharedaccountability/glance/)
b. Yes, this includes staff and students.
c. Anticipated future enrollment projections available on the website https://www.montgomeryschoolsmd.org/school-profiles
d. Yes

Question 41: **Section 3.2: On User Mobility & Chromebooks: "The RFP notes a 'Chromebook heavy environment.' How do you plan to provide consistent security policy and a fast user experience for students and staQ when they take those devices home or use them oQ-campus? How will a site- based firewall provide coverage for these oQ-network users?" Are these Chromebooks used by students and staQ? Are you looking to secure these Chromebooks when they are oQ-premise and remote?**

Answer 41: **Section 3.2**

a. Mobile security is currently provided by the extension within the user session, regardless of location. MCPS is seeking vendor recommended solutions and vendors need to respond with what they can do.
b. This would be supplemental while on site, not related to off-campus.
c. Chromebooks are used by both staff and students.
d. Yes

Question 42: **Section 3.3: ZTNA remote access – how many users? Only for remote or also ZTNA when at school?**

Answer 42: ZTNA for all remote users. No for remote and potentially for at school.

Question 43: **Section 3.3: Can you clarify? Are all users on managed devices? Or are some users using unmanaged devices?**

Answer 43: No, Some remote access users (e.g. contractors) are on unmanaged devices.

Question 44: **Section 3.3: Remote access – where are the systems/apps people are accessing? In data centers, public cloud (AWS, Azure, GCP), co-loc?**

Answer 44: Remote access users are currently fully tunneled so the access is to everything, including local DCs, public cloud, other internet hosted.

Question 45: **Section 4.1: On High Availability (HA): " How do you define High-Availability? What are your requirements for HA in general?**

Answer 45: MCPS defines HA in the same general definition used by the industry. MCPS would like a solution that can trigger a failover event not just based off interface(s) status but environmental conditions as well. We prefer a solution that can-do HA while pairs are not physically in the same location.

Question 46: **Section 4.1: Mentions zero trust readiness. Is there a zero-trust strategy and if so, can it be shared?**
Answer 46: MCPS is seeking vendor recommended solutions and vendors need to respond with what they can do.

Question 47: **Section 4.2: On "Cloud OQloading": "Section 4.2 mentions an 'option for extending services through cloud oQloading.' What specific services or traQic types are you envisioning for cloud oQloading, and what outcomes are you hoping to achieve?"**
Answer 47: We already have a great deal of our systems offloaded to the cloud, we are exploring the possibility of also offloading security services to the cloud.

Question 48: **Section 7: Evaluation criteria – do you plan on testing solutions before making an award?**
Answer 48: No

All responses to the Form 470 and RFP must be submitted electronically to Saudy_EspinalDeVeloz@mcpsmd.org no later than 2:00 p.m. Eastern time on October 23, 2025. The MCPS Procurement website address is www.montgomeryschoolsmd.org/departments/procurement/. Late proposals will not be considered.

Saudy Espinal
____
Saudy Espinal DeVeloz, Buyer II, Department of Procurement

Please indicate your acceptance of this notice by signing below and returning with your response to the Form 470 or under separate cover.

Accepted:

____
Name and Title

____
Company Name

Copy to:
RFP File