LEGAL ADVERTISEMENT

Notice is hereby given that the Board of School Trustees of the MSD Pike Township, 6901 Zionsville Rd, Indianapolis, IN shall receive sealed Request for Proposals for the Cybersecurity Pilot – Next Generation Firewall Project.

A 470 has been posted for the MSD Pike Township for the purpose of Cybersecurity Pilot – Next Generation Firewall Project through the FCC's Cybersecurity Pilot Project federal E-Rate Program. Please check the USAC website for the 470 posting. Reference 470 # CBR420250281 .

Bids must be submitted in a sealed envelope with a return address, plainly marked on the outside; CYBERSECURITY PILOT. All bids shall be in compliance with the laws governing such matters and the Board reserves the right to reject any and all bids and to waive any formality in the process.

Bid documents are to be submitted by 2:59 PM on June 9, 2025:

MSD Pike Township

Attention: CYBERSECURITY PILOT

6901 Zionsville Road

Indianapolis, IN 46268

Board of School Trustees

MSD Pike Township

MSD Pike Township

Request for Proposals – MSD Pike Next Generation Firewall – Cybersecurity Pilot 2025(MSD Pike NGFW CP 25)

April 25, 2025

Overview

The Metropolitan School District of Pike Township is an award winning school district, widely regarded as an education leader for high academic standards, innovative educational programs, state-of-the-art facilities, strong parental and community partnerships, exceptional students, and acclaimed educators. Our district is comprised of nine elementary schools; Central Elementary School, College Park Elementary School, Deer Run Elementary School, Eagle Creek Elementary School, Eastbrook Elementary School, Fishback Creek Public Academy, Guion Creek Elementary School, New Augusta Public Academy South, and Snacks Crossing Elementary School, which serve students in kindergarten through 5th grade. Our three middle schools; Guion Creek Middle School, Lincoln Middle School, and New Augusta Public Academy North, serve students in 6th through 8th grade. We also have an independent Freshman Center at Pike High School. In addition, the Pike Preparatory Academy serves middle school scholars in need of additional support in the areas of behavior and/or academics, and high school students who benefit from an alternative learning environment.

The **MSD of Pike Township** (the "Applicant") is seeking proposals for a project to supply and install a Next Generation Firewall. Bidders are advised that this project will be contingent upon the "district" successfully obtaining funding from USAC Cybersecurity Pilot program. The contract agreement between the district and the successful bidder must recognize that contingency.

The Applicant seeks an agreement that allows it to work with the selected vendor to adjust quantities and/or scale back or cancel the project entirely as needed based upon funding availability and/or the best interests of the Applicant.

Project Scope

The Applicant seeks eligible equipment as outlined in Appendix A. Equipment shall be new, factory-sealed equipment currently available from the manufacturer; the Applicant will not accept proposals of used, remanufactured, refurbished, "B stock," returns, open-box, discontinued, "gray market," or equipment in any other condition other than new and factory-sealed with all original manufacturer warranties.

Installation will be in place of existing equipment and the requested equipment will be integrated into the existing environment. Each bid should include all labor necessary for staging, installation, testing, and documentation of equipment. Equipment staging will consist of (but not be limited to) ensuring firmware version consistency, configuration loading, and hardware preparation for mounting. Software and firmware version for components will be agreed upon at time of deployment, and configurations will be coordinated with the Applicant's staff. Installation by the selected vendor shall include the removal of the existing equipment and placement of the new equipment. Equipment testing should verify access to internal resources and the Internet. Documentation should include configuration and summary reports of installations.

Proposals should include pricing for an appropriate number of hours of onsite professional training that is manufacturer-specific basic instruction on the use of eligible equipment. The training should be directly associated with equipment installation, and part of the contract or agreement for the equipment being proposed.

Site Visit

A **voluntary** site visit will be held at the Pike Freshman Center, 6801 Zionsville Road, Indianapolis, IN at 1:00p.m on Monday, May 19, 2025. This will be the only opportunity to ask questions or to receive answers to questions related to this RFP. Respondents choosing not to attend in so doing acknowledge their understanding that they were offered and voluntarily declined the opportunity.

Response Format

Responses should include the following, if applicable:

- Applicable items should include all related software and hardware components that enable the functionality of the equipment (including any necessary mounting brackets, software licenses, multi-year licenses, and basic maintenance).
- If applicable, vendor is to specify all fees, shipping charges, taxes, surcharges and contingency fees for eligible equipment.
- If applicable, vendor is to specify the manufacturer's warranty provided as an integral part of an eligible component without separately identifiable cost.
- Any ongoing subscription pricing must be listed separately.

Your response **must** include the following information:

1. Line-item pricing for each item listed in Appendix A. Any discounting applied to your proposal must be reflected at the line-item level.
2. In the case of proposed equivalent products, a thorough technical description of how each product from the manufacturer being bid meets each of the required functionalities of the product listed herein.
3. Information outlining your company's certifications and connections regarding the manufacturer's equipment being bid, and length of time your company has provided equipment from the manufacturer being bid.
4. Two (2) reference sites where your company has performed a similar installation of the equipment being bid, including business name, contact name and contact information. It is preferable that at least one reference should be for a school corporation or library system within 90 miles of the Applicant.
5. Your USAC SPIN Number. (You must have a current SPAC form on file with USAC.)
6. A ready to execute contract which includes the proposal requirements and the Cybersecurity Pilot contingencies outlined herein.
7. A ready-to-execute contract which includes the proposal requirements and the Cybersecurity Pilot contingencies outlined herein. If the bidder plans to seek progress payments during the course of this project, the contract must clearly indicate what the progress milestones will be and invoices must specifically describe which of the contracted milestones are being billed.

The Applicant's review of information will be primarily focused on the substance of the details provided in response to the requirements herein including but not limited to technical details, pricing and terms, experience, references, and adherence to the response format provided. Per E-rate rules, the cost of eligible goods and services will be the most heavily weighted evaluation factor.

Proposals must be prepared with specificity with regard to the equipment and/or services listed herein. *Bids merely listing a general menu of equipment and/or services available from a vendor, bids appearing to be automatically generated without specificity in relation to the requirements of this RFP, and bids missing substantial information but inviting the applicant to contact the bidder to refine the bid and/or discuss specifics will not be considered valid bid responses and will be disqualified from consideration. This includes any SPAM and/or robotic responses.* For more information, please review the USAC E-Rate News Brief of February 15, 2024.

Proposal Delivery and Opening

The Applicant reserves the right to reject each and every bid, and to waive informalities, irregularities, and errors in the bidding to the extent permitted by law. This includes the right to extend the date and time for receipt of bids. In the event that a responsible bid is not received or if it is determined that the low bid received is too high, the bid received will be rejected and the project will be cancelled or re-bid.

Sealed bids should be delivered to 6901 Zionsville Road, Indianapolis, IN by 2:59 PM on June 9, 2025. Bid opening will begin promptly at 3:00 PM.

Mailing address:

MSD Pike Township
ATTN**: Cybersecurity Pilot**
6901 Zionsville Road
Indianapolis, IN 46268

APPENDIX A – Next Generation Firewall Requirements

Below is a reference of the type of equipment and capacities (or their equivalent) to be supplied. Bidders should price separately and clearly indicate any ineligible costs for all services and equipment associated with this RFP. For any part numbers that have been updated or replaced by the manufacturer, bidders should offer the most similar current part.

A. GENERAL REQUIREMENTS

The MSD of Pike is seeking to upgrade or replace its current firewall solution with next-generation firewall hardware, software, support, and related services. The objectives of the proposed solution are as follows:

Full Data Inspection (Deep Packet Inspection): Provide comprehensive inspection services for all inbound and outbound traffic with a minimum combined throughput of 40 GBs.

Application Identification and Control: Identify and manage applications based on their characteristics, regardless of their ports, encryption, or evasive techniques.

Threat Protection: Safeguard the district's users, network, and data from both internal and external threats.

Firewall Policies: Develop firewall policies based on the authentication of internal users and devices.

Integration: Ensure seamless integration with the district's existing hardware, software, and Endpoint Detection and Response (EDR) solution.

AI-Driven Threat Intelligence: Utilize real-time AI-driven threat intelligence to enhance security measures.

1. CONNECTIVITY AND HARDWARE REQUIREMENTS

- Throughput: Support a minimum sustained throughput of 40 Gbps with all threat management extensions enabled. The proposed firewall solution must be scalable to accommodate the school division's growing needs and higher throughput requirements.
- Ports: Each firewall must include at least five (5) 10 Gbps SFP+ ports. Additional ports and the ability to utilize QSFP+ are desired. All ports must be compatible with the existing network equipment.
- Hardware Compatibility: Ensure compatibility with 60km SFP+ modules that support single-mode fiber (SMF).
- Power Supply: Provide a modular hot-swappable (1+1) dual power supply.
- Storage: Preferably utilize solid-state hard drives (SSD) with sufficient storage to retain operational data on the device for at least 6 months.
- Protocol Support: Support dual stacking of IPv4 and IPv6 protocols for all firewall features and functions.
- Platform Compatibility: The proposed solution must support platforms including Windows operating system, Linux operating system, and all virtual environments, including but not limited to VMWare, Azure, and Hyper-V.
- Security Features: Support stateful protocol filtering, deep packet inspection, and detection of attacks within the payload.
- Micro-Segmentation: It is desired that the proposed solution provides micro-segmentation capabilities to block the lateral movement of nefarious network traffic in the data center network.

2. FIREWALL MANAGEMENT

- Compliance: The proposed solution must be fully compliant with CIPA, COPPA, HIPAA, and PCI standards.
- Centralized Management: The solution must be manageable via a single management console for all included features.
- Firewall Rule Verification: The solution should notify the administrator when a new rule masks, duplicates, overlaps, or interferes with existing configurations.
- Encryption: Communication between management servers, interfaces, and all appliances must be encrypted.
- Device Monitoring: The solution must offer real-time monitoring, proactive alerts, historical reporting, and troubleshooting tools, preferably utilizing artificial intelligence (AI) or cloud-based technologies.
- Automation: The solution should provide the ability to automate routine tasks and drill-downs to maximize efficiency with minimal effort.
- Administrator Management: The solution must support user delegation based on roles, permissions, and endpoint groupings for effective management.
- Log Analysis: The solution must include features to search, analyze, and visualize data to obtain operational insights. Proposals should include a detailed explanation of the various types of log analysis that can be compiled through the solution.

3. USER IDENTITY AND REPORTING

- Authentication and Security Methods: The solution must support multiple authentication and security methods, including local user databases, TACACS+, Microsoft Active Directory, Microsoft Azure Active Directory, LDAP-compliant directory, Radius, and Google SAML.
- Active Directory and Google Integration: Provide an interface to Active Directory (AD) and Google to pull user IDs and groups for use in firewall rules. Must support cloud connectivity on Azure Active Directory.
- Integrated and Customizable Search: Offer integrated and customizable search capabilities to search data from all systems for information relevant to incident investigations or risk analysis.
- Manual and Scheduled Scans: Provide manual and scheduled scans of specified systems for indicators derived from threat intelligence or other sources.
- Integrated Analytics: Include integrated analytics (including visualization) and support the creation of custom analytics to identify anomalous endpoint behaviors, support incident investigation, and perform event analysis.

4. THREAT MANAGEMENT

- Segmentation: The solution must segment the server/service infrastructure from internal and external threats.
- Application Control: Identify and manage user network application activity based on users, groups, or IP ranges.
- URL Filtering
    - Categorize and filter URLs to block, allow, and limit available bandwidth based onURL categories and/or reputation
    - Protect against web-based phishing, malware, and command-and-control
    - Offer granular filtering controls for individual users, groups, applications, and network ranges
    - Log all URLs passing through the filter, both blocked and permitted, and provide a history/report of URLs accessed by users over a certain period
    - Allow users to submit URLs that may be miscategorized
- SSL Decryption: Support SSL decryption.

- IoT Security: It is desired that the solution offers threat protection for IoT devices.
- DNS Security: It is desired that the solution offers threat protection from DNS and malicious domain-based attacks.
- Threat Intelligence: Integrate with vendor and/or third-party threat intelligence databases. Please describe how this information is obtained, managed, and updated within the solution, and specify any additional components needed for this feature.
- 3rd Party Antivirus: Seamlessly integrate with the school division's existing desktop and server antivirus solutions.

5. SUPPORT

- Manufacturer's Multi-Year Warranty: A manufacturer's multi-year warranty for a period up to three years that is provided as an integral part of an eligible component, without a separately identifiable cost, may be included in the cost of the component
- 24x7x365 Support: Provide manufacturer 24x7x365 dial-in support for all features with an initial response time of one hour or less. Please include details about the multi-year warranty.
- Return Merchandise Authorization (RMA): Provide RMA for defective/failed equipment.
- Maintenance and Support Pricing: Specify pricing for any additional maintenance and support for hardware and/or software, including options for 1-, 3-, and 7-year renewals.
- Product Roadmap: Provide a five-year product roadmap, ensuring all proposed systems and sub-components are not End-of-Life for at least seven years.

6. OTHER REQUIREMENTS

- System Configuration: Assist in the setup, configuration, and optimization of the management solution.
    - Migration: Migrate all current firewall settings, network configurations, rules, policies, and other information from the current firewall solution.
    - Documentation: Provide a list of printed documentation for the operation, use, and administration of the implemented solution.
- Compliance an
    - National Security Compliance: Ensure the solution does not involve any company posing a national security threat to the integrity of communications networks or the communications supply chain. See USAC Supply Chain for more details.
    - Lowest Corresponding Price (LCP): As required by Cybersecurity Pilot rules, all proposals in response to this Form 470 must offer the Lowest Corresponding Price ("LCP"). See USAC Cybersecurity Pilot for more details.