Cybersecurity RFP Vendor Questions & Responses

This document provides responses to questions submitted by vendors regarding the current RFP. The responses are intended to clarify requirements, scope of work, and expectations.

Overview

Client	Clarksdale Municipal School District
Project	Cybersecurity Infrastructure Modernization
Project Manager's Name	Amanda S. Bell. Director of IT
Project Manager's Email	amanda.s.bell@cmsd.k12.ms.us
Description	Clarksdale Municipal School District (CMSD) invites qualified vendors to submit proposals for the design, deployment, and support of a cybersecurity infrastructure solution. This project is supported by CMSD's recent award from the FCC Cybersecurity Pilot Program and is designed to strengthen identity protection, patching processes, endpoint visibility, and security event detection capabilities across the district. The awarded solution must include secure identity services, patch management, endpoint protection, privilege misuse monitoring, and centralized detection and response capabilities.
Anticipated Project Start Date	October 1, 2025
Key Resources	• Clarksdale Cyber Security Pilot RFP • Addendum NO. 2 Clarksdale Cybersecurity RFP

Vendor Questions and Responses

Question	Answer
Q1: What systems/platforms will need to be protected by MFA?	A1: All administrative access points, including email, district servers, and critical applications, must be protected by MFA.

Q2: Does the district intend to manage their own EDR/XDR or have it managed for them?	A2: The district is open to both options and requests vendors to provide pricing for self-managed and fully managed solutions.
Q3: How many endpoints are on the network that need EDR protection and what operating systems do they have?	A3: Approximately endpoints, consisting of Windows PCs, laptops, and a smaller number of MacBooks. Laptops/PC: 500 Desktops: 200+ Servers: 7 Chromebooks: 2000
Q4: Is a fully managed firewall an option as well?	A4: No, the district has a fully managed firewall.
Q5: Do you need vulnerability assessments of internal or external threats or both?	A5: Both. The district requires regular vulnerability assessments of internal and external threats.
Q6: Is there a SIEM or SIEM service in place now?	A6: No, this RFP includes the acquisition and configuration of a SIEM solution.
Q7: Are the 3 K-12 references with similar projects a hard requirement?	A7: Yes, they are.
Q9. Do you need DLP for data in cloud storage like Google Workspace?	Yes. The district requires DLP capabilities for cloud-based storage, particularly Google Workspace, to prevent unauthorized sharing, downloading, or exfiltration of sensitive data. System currently in place- ManagedMethods
Q10. DNS-Layer Filtering & threat prevention - Please elaborate on the need above as DNS filtering is typically performed during firewall inspection.	The district requires DNS-layer filtering as an additional layer of protection beyond traditional firewall inspection. This will allow proactive blocking of known malicious domains, phishing sites, and command-and-control callbacks, particularly for remote and roaming devices that may bypass the district firewall.

Key Information and Updates

Updated Section 11. Timeline (Page 5)

Milestone	Date
RFP Release	August 12, 2025
Questions Due	September 1, 2025
Responses to Questions Posted	September 3, 2025 **(All questions received, and answers will be posted to the District website)**
Proposal Submission Deadline	September 15, 2025
Vendor Selection & Notification	September 15, 2025
Anticipated Project Start	October 1, 2025

Original Section 12. Submission Instructions (Page 6)
Submit proposals electronically via email to:
Amanda Bell
Technology Coordinator
abell@cmsd.k12.ms.us
Subject: "Cybersecurity RFP Response - [Your Company Name]"

Updated Section 12. Submission Instructions (Page 6)

Bids may be hand delivered or mailed to the Clarksdale Municipal School District located at 526 South Choctaw Street, Clarksdale, MS 38614.

Bids must be submitted in a sealed envelope clearly marked as follows:

ATTN: SEALED BID - DO NOT OPEN
"2025 Cybersecurity Bid"
Bid Opening: September 15, 2025, 10:00 a.m.

Envelopes not so marked will not be considered. The Clarksdale Municipal School District Board of Trustees reserves the right to reject any and/or all bids and waive any informality.

As an alternate submission mechanism for Cybersecurity products and services, bids may be submitted through secure electronic submission. Official Bid Documents are available at Central Bidding (www.centralbidding.com). Electronic Bids may be submitted at Central Bidding (www.centralbidding.com). For questions related to the electronic bidding process, please call Central Bidding at 225-810-4814.

Bidders must submit one (1) original and two (2) copies of their full response along with two (2) electronic copies.

DO NOT FAX OR EMAIL PROPOSALS. FAXED OR EMAILED PROPOSALS WILL BE DISQUALIFIED.

The submission of automated or “robo” bids or proposals will be automatically disqualified. To be clear, “SPAM and/or robotic responses will not be considered valid bid responses and will be disqualified from consideration.”