St. Mary Parish School District
Request for Proposal

Schools and Libraries Cybersecurity Pilot Program

RFP Number: Cybersecurity 2025

Proposal Deadline

June 17, 2025 2:00 PM

(CST) Event Calendar

EVENT	DATE	TIME	LOCATION
Release RFP	**April 23, 2025**	**2:00 PM (CST)**	**EPC, Central Bidding**
Virtual Pre-Bid Conference (Mandatory)	**May 12, 2025**	**10:00 AM (CST)**	**Virtual Conference See Page 20**
Q and A Open	**May 12, 2025**	**2:00 PM (CST)**	**erate@st.maryk12.net**
Q and A Closes	**May 28, 2024**	**2:00 PM (CST)**	**erate@st.maryk12.net**
Submission Deadline	**June 17, 2025**	**2:00 PM (CST)**	**St. Mary Parish School Board**

ST. MARY PARISH SCHOOL DISTRICT ("DISTRICT") reserves the right to reject all proposals and to waive any formality defects or clerical errors in any Bid Proposal Package, in the interest of the district.

NOTICE TO SERVICE PROVIDERS

Cybersecurity Pilot Program

St. Mary Parish School District is seeking bids from **qualified** Cybersecurity Service providers to submit proposals for Cybersecurity services and equipment. The Cybersecurity Pilot Program is a significant initiative, and St. Mary Parish School District is one of 645 applicants selected from the United States and its Territories to participate in this crucial program.

The Schools and Libraries Cybersecurity Pilot Program provides up to $200 million to selected participants over a three-year term. This substantial funding can be used to purchase a wide variety of eligible cybersecurity services and equipment, offering a significant opportunity for the selected schools and school districts.

Selected school districts and libraries are eligible to receive up to $13.60 per student, annually, on a pre-discount basis, to purchase eligible cybersecurity services and equipment over the three-year Pilot duration. Currently, St. Mary has an enrollment of 8,461 students.

Vendors will need to review the FCC Guidance about the Cybersecurity Pilot Project to bid on the project successfully.

Bids may be uploaded to http://centralauctionhouse.com. (Please check the site in ADVANCE for rules and fees for uploading to the bidding site(s). Submissions must be received on or before June 17, 2025, at 2:00 PM (CST).

If delivered, sealed proposals should be sent via certified mail, UPS, FedEx, or hand-delivered to:

St. Mary Parish School District

Attn: Kaylum Vead, IT Director

212 Onstead Street

Morgan City, Louisiana 70380

PROPOSAL DEADLINE IS JUNE 17, 2025, AT 2:00 PM

TABLE OF CONTENTS

TERMS AND DEFINITIONS

TERMS	DEFINITION
ADDENDUM	A Document or information attached or added to clarify, modify, or support the information in the REQUEST FOR PROPOSAL. All addenda will be uploaded to the E-Rate Portal (EPC) and, if required, to the electronic bidding site.
ADMINISTRATIVE REVIEW	The district's final review by the administrative authority determines whether a bid complies fully with the Request for Proposal (RFP) or not. Bids may be disqualified for reasons outlined in the RFP.
AGREEMENT	A contract that has been agreed upon and signed by THE DISTRICT. Sometimes, the agreement will be a letter of award, a purchase order, or another legally binding document, pending final signatures.
ASSIGNMENT OF CONTRACT OR PURCHASE ORDER	The bidder(s) shall not assign or transfer by law or otherwise any rights, burdens, duties, or obligations without the prior written consent of THE DISTRICT. This includes corporate takeovers, buyouts, or mergers.
BEST AND FINAL OFFER	THE DISTRICT reserves the right to conduct a BAFO with one or more Proposers determined by the evaluation committee to be reasonably qualified to be selected for award. If selected, the Vendor(s) will receive written notification of their selection, along with a list of specific items to be addressed in the BAFO and instructions for submittal. The BAFO negotiation may assist THE DISTRICT in clarifying the scope of work or obtaining the most

	cost-effective pricing from the Proposers. The evaluation criteria for a BAFO will be the same as used in the initial scoring rubric.
BID	The Vendor's Response to the Request for Proposals.
CONFLICT OF INTEREST	A Conflict of Interest shall exist when a Vendor or any affiliated person or business entity provides goods or services under a Contract Award whereby one or more personal, business, or financial interests or relationships exist which would cause a reasonable individual with knowledge of the relevant facts to question the integrity or impartiality of those who are or will be acting on behalf of THE DISTRICT.
CONTRACT AWARD	The acceptance of a Quote, Bid, Proposal, or Offer; a Purchase Order, Contract Agreement, or other formal notification of award issued by an authorized official of THE DISTRICT. The term 'contract award' refers to formally notifying the vendor that they have been selected as the supplier for a particular contract.
CONTRACT TERM	The terms of a Contract or Agreement will be available for use by THE DISTRICT. Voluntary extensions may be available as an option to extend the contract term.
DEFAULT BY CONTRACTOR	THE DISTRICT shall hold the bidder(s) responsible for any damage that may be sustained due to failure to comply with any terms or conditions listed in the RFP or resulting contract. It is specifically provided and agreed that time is of the essence in meeting the contract delivery requirements. If the successful bidder(s) fails to deliver services listed herein at the prices named and at the time and place herein stated or otherwise fails or neglects to comply with the terms of the bid, THE DISTRICT may, upon written notice to the bidder, cancel the contract in its entirety or cancel or rescind any or all items affected by such

	default, and may, cancel the contract in whole or in part. THE DISTRICT may consider the second winner or re-advertise the position. If all the original proposers are unable to provide the services, the district will seek a well-qualified, good Samaritan Telecommunications Company to accept the agreement under the same terms.
EQUIVALENT	A replacement for a good or service that achieves the same result and has the same functionality as the product or service requested in the RFP. All equivalent goods and services will be considered that meet the definition.
INVOICES AND PAYMENTS	All vendors submitting proposals must agree to invoice THE DISTRICT according to their preferred billing method: SPI or BEAR. For all SPI invoices, the Funding Request Number (FRN) for each service, the total monthly cost, the discount portion owed by THE DISTRICT, and the amount billed to USAC must be displayed on the invoice.
NOTICE OF INTENT AWARD	A formal, written document issued by an authorized official of THE DISTRICT informing a Vendor that a Contract has been awarded to the Vendor based on its Solicitation Response. In some cases, the approval of the finance committee, THE DISTRICT board, and/or other authorizing bodies is required to finalize the agreement.
TERMINATION OF AGREEMENT	Any person aggrieved in connection with the solicitation or award of a contract shall protest to THE DISTRICT. A Protest concerning a solicitation shall be submitted in writing at least two (2) days before the opening of bids. A Protest concerning the award of a contract shall be submitted in writing within fourteen (14) days after the contract award. THE DISTRICT may terminate agreements upon giving thirty days' advance written

	notice of intent to terminate the contract for good cause. (e.g., failure to deliver services, failure to comply with the conditions and specifications within the RFP).
FCC CYBERSECURITY PILOT PROJECT	The FCC's Schools and Libraries Cybersecurity Pilot Program is a three-year, $200 million initiative that provides funding for eligible K-12 schools and libraries to enhance their cybersecurity services and equipment, to protect their broadband networks and data from cyber threats.

I. BACKGROUND

Pilot funds will be available as soon as the Pilot applicant receives a funding commitment decision letter (FCDL) from USAC. Unlike the E-Rate program, the Pilot does not utilize specific funding years; therefore, participants do not need to wait until a specific date (e.g., July 1, 2025) to purchase cybersecurity equipment and services, provided they have otherwise completed the requirements and received funding commitment decisions. Pilot participants and service providers will be eligible to request reimbursement after receiving or delivering eligible cybersecurity services and/or equipment through the Pilot Program.

Funding can be utilized under the Cybersecurity 3-year plan and is only limited to the overall budget. Applicants will pay a match equal to the applicants' Category 1 budget.

Once a Pilot participant receives an FCDL committing funding for eligible services and/or equipment, they may begin submitting reimbursement requests (i.e., FCC Form(s) 472/474) after receiving or delivering the requested services and/or equipment.

As in the E-Rate program, USAC will review and process requests for reimbursement in batches and submit them for approval to the Commission. Disbursements are then made through the Department of the Treasury. Upon receiving or delivering the requested services and/or equipment, the service provider will invoice using the Service Provider Invoice (SPI). Applicants may opt for the BEAR form.

USAC will review and process reimbursement requests in batches and submit them for approval to the Commission. Disbursements are then made through the Department of the Treasury.

II. ELIGIBLE EQUIPMENT AND SERVICES

A. Advanced/Next-Generation Firewalls

Equipment and services that implement advanced or next-generation firewalls, including software-defined firewalls and Firewall-as-a-Service, are eligible for consideration. Specifically, equipment, services, or a combination of equipment and services that limit

access between networks, excluding basic firewalls that are funded through the Commission's E-Rate program, are eligible.

Eligible equipment and services may include the following features, substantially similar features, or their equivalents:

B. Advanced Threat Detection and Prevention

AI/ML Threat Detection and Response

Application Awareness & Control

Cloud-Delivered Threat Intelligence

Comprehensive Network Visibility Software-defined Firewalls

Deep Packet Inspection (DPI)

Distributed Denial of Service (DDoS) Protection

Firewall as a Service (FWaaS)

Integrated Intrusion Prevention Systems (IPS)

Internet of Things (IoT) Security

Intrusion Prevention/Detection

Malware Detection

Network Segmentation

Patch Management Systems

VPN

C. Endpoint Protection

Equipment and services that implement endpoint protection are eligible for consideration. Specifically, equipment, services, or a combination of equipment and services that implement safeguards to protect school- and library-owned end-user devices, including desktops, laptops, and mobile devices, against cyber threats and attacks are eligible.

Eligible equipment and services may include the following features, substantially similar features, or their equivalents:

- Anti-Malware
- Anti-Ransomware
- Anti-Spam
- Anti-Virus
- Endpoint Detection & Response (EDR)
- Extended Detection & Response (XDR)
- Insider and Privilege Misuse
- Privileged Access Management
- Secure Sockets Layer (SSL) Inspections
- Target Intrusions
- Web Application Hacking

D. Identity Protection and Authentication

Equipment and services that implement identity protection and authentication are eligible for consideration. Specifically, equipment, services, or a combination of equipment and services that implement safeguards to protect a user's network identity from theft or misuse, and/or assure the network identity of an entity interacting with a system, are eligible.

Eligible equipment and services may include the following features, substantially similar features, or their equivalents:

E. Active Countermeasure Tools

Cloud Application Protection

Cloud Services

Credential Stuffing

Content Blocking and Filtering/URL Filtering

Content Caching Systems and Service

Customer Portal Services

Digital Identity Tools

Distributed Denial of Service (DDoS) Protection

DNS/DNS-Layer Security, Blocking, and Filtering

Email and Web Security

Identity Governance & Technologies

Intrusion Detection Systems (IDS)

Logging Practices / Event Logging

Network Access Control

Offsite/Immutable back-ups

MFA/Phishing-Resistant MFA

Patching

Password Spraying

Privileged Identity Management

Products with TPM Chips

Secure Access Service Edge (SASE)

Secure-By-Design Equipment and Services

Security Information and Event Management (SIEM)

Security Updates

Single Sign-On (SSO)

Trusted Platform Module (TPM)

Web Content Controls

Wireless Access Controllers

Zero Trust Architecture

F. Monitoring, Detection, and Response

Equipment and services that implement monitoring, detection, and response are eligible. Specifically, equipment, services, or a combination of equipment and services that monitor and/or detect threats to a network and that take responsive action to remediate or otherwise address those threats are eligible.

Eligible equipment and services may include the following features, substantially similar features, or their equivalents:

- ✓ Advanced Attack Surface Management and Asset Management Solutions
- ✓ Bug Bounty Solutions & Services
- ✓ Compliance Assessment
- ✓ Dark Web Scanning
- ✓ Data Loss Prevention
- ✓ Internal/External Vulnerability Scanning
- ✓ Network/Device Monitoring & Response
- ✓ Network Security Audit
- ✓ Network Traffic Analysis
- ✓ Managed Detection & Response (MDR)
- ✓ Managed Service Providers
- ✓ Maturity Models
- ✓ Network Detection Response (NDR)
- ✓ Penetration Testing
- ✓ Security Operations Center (SOC) for Around-the-Clock (24/7/365) Monitoring, Detection, and Response
- ✓ Threat Hunting/Updates and Threat Intelligence
- ✓ Vulnerability Management

Notes:

Certain technologies (e.g., DDoS protection) are listed in multiple categories above, reflecting their categorization in the marketplace from multiple perspectives.

Eligible costs include maintenance, operation, and support charges, as well as monthly charges, special construction, installation, and activation charges, software, modulating electronics, and other equipment necessary to make the eligible equipment and services functional. All eligible equipment, services, and related costs, including maintenance and operation, must be competitively bid.

A manufacturer's multi-year warranty, provided as an integral part of an eligible component and lasting up to three years, may be included in the component's cost without a separately identifiable charge.

Eligibility is limited to equipment that is network-based (i.e., that excludes end-user devices, including, for example, tablets, smartphones, and laptops) and services that are network-based and/or locally installed on end-user devices, where the devices are owned or leased by the school or library, and where equipment and services are designed to identify and/or remediate threats that could otherwise directly impair or disrupt a school's or library's network, including to threats from users accessing the network remotely.

G. Ineligible costs include:

Any equipment, service, or other related cost that is eligible in the Commission's E-Rate eligible services list program in the funding year for which Pilot reimbursement is sought.

Any equipment, service, or other related cost for which a participant has already received reimbursement, or plans to apply for reimbursement, through any other USF or federal, state, or local program in the funding year for which Pilot reimbursement is sought.

Staff salaries and labor costs for personnel of the participant or underlying beneficiary are not eligible.

Consulting services that are not related to the installation and configuration of the eligible equipment and services are not eligible. These include services related to application

assistance, Program advice, and other activities not directly tied to the actual installation and initial configuration of eligible equipment and services.

Long-term planning and risk assessment surveys, including threat intelligence analysis and costs associated with incident response plans

Security cameras, asset tracking tags, insurance costs, threat response exercises, training, and any costs associated with responding to specific ransom demands are ineligible.

Any equipment or services prohibited by the Secure and Trusted Communications Networks Act of 2019, Pub. L. No. 116-124, 134 Stat. 158 (2020) (codified as amended at 47 U.S.C. §§ 1601–1609) (Secure Networks Act) or the Commission's rules, including Commission rules 54.9 and 54.10, that implement the Secure Networks Act.

H. Training

Training is eligible as part of the installation of the equipment and services only if it is basic instruction on the use of eligible equipment and services, directly associated with the equipment and services installation, and is specified in the contract or agreement for the equipment and services. Training must occur coincidentally or within a reasonable time after installation.

III. SCOPE OF WORK

I. GOALS AND OBJECTIVES

Develop/implement/improve security and protection of E-Rate-funded broadband network(s)

☑ Develop/implement/improve network and data monitoring

☑ Develop/implement/improve incident detection and response

☑ Develop/implement/improve protective controls

☑ Develop/implement/improve user access control

☑ Obtain/supplement the cost of third-party cybersecurity management assistance

J. EXPECTATIONS

Note: substantially similar features, or their equivalents, of any manufacturer or software brand requests will be considered.

Security and Protection of E-Rate-Funded Network:

The project will enhance the district's network security by deploying Network Access Control (NAC), ensuring real-time protection against unauthorized users who may introduce malware and ransomware onto the network.

Network and Data Monitoring: Cyber Storage NAS DLP will continuously monitor the network for unauthorized data movement and cyber threats, enhancing overall visibility and protection.

Protective Controls: PAM will enhance user access control and privilege management to mitigate risks associated with insider misuse.

User Access Control: PAM will manage privileged accounts, enforcing strict access controls to sensitive data and systems.

K. SECURITY LIFECYCLE REPORT (SLR)

St. Mary Parish School District included a Security Lifecycle Report as part of the documentation submitted with the initial FCC application. The report's findings will be used to assist service providers in preparing a proposal (See Appendix A)

The proposed cybersecurity project for the St. Mary Parish School Board aims to address critical vulnerabilities identified in the network through the Schools and Libraries Cybersecurity Pilot Program. The Security Lifecycle Report (SLR) conducted by Palo Alto Networks revealed significant cybersecurity challenges that require immediate action to protect the district's broadband network and sensitive data.

L. Cybersecurity Issues and Challenges

- Vulnerability Exploits: 2,904,574 detected vulnerability exploits targeting critical applications like Active Directory and Microsoft SMB.

- Total Threats: Over 11 million threats, including malware, command-and-control (C2) traffic, and malicious file transfers.
- High-Risk Applications: A total of 28 high-risk applications were identified, including file-sharing and encrypted tunneling apps.
- Command-and-Control Communications: 8,628,332 C2 requests indicating malware communication attempts.
- Malicious Web Requests: 850 malicious URL requests were identified, including phishing sites and malware delivery platforms.

M. Proposed Cybersecurity Action Plan

Note: substantially similar features, or their equivalents, are allowable

Data Loss Prevention and Monitoring with Cyber Storage NAS and Zerto CDP

To protect sensitive data from unauthorized access and exfiltration, the district will deploy a Cyber Storage NAS data loss prevention (DLP) solution in conjunction with Zerto for continuous data protection, disaster recovery, and real-time monitoring, under the category of Monitoring, Detection, and Response. Monitoring will provide real-time protection and a zero-trust data environment, while Zerto will offer continuous data protection and replication for fast recovery in the event of a breach or ransomware attack, resulting in the fastest RTO and RPO.

Network Access Control (NAC) is a security approach that restricts access to private networks and sensitive resources by enforcing policies on endpoints, ensuring only authorized and compliant users and devices are allowed to connect. It serves as a digital gatekeeper to enhance security, compliance, and network integrity. The district plans to incorporate this technology to prevent unauthorized access to the network.

In December 2023, the district was impacted by a Cyberattack. HPE Aruba ClearPass NAC did not function properly and was removed from the district's environment. The renewal is scheduled for 2026, and the district plans to reinstall, reconfigure, and renew for this pilot. A properly functioning NAC is a critical part of our cybersecurity posture improvement plan.

Privileged Access Management (PAM)

Note: substantially similar features, or their equivalents, are allowable

The district will implement a Privileged Access Management (PAM) solution to manage privileged accounts and enforce access controls for sensitive systems and applications. This will reduce the risk of insider threats and unauthorized access to critical data by automating credential management and auditing privileged sessions.

N. Additional Key Initiatives:

Endpoint Detection and Response (EDR)

The project will leverage the existing Endpoint Detection and Response (EDR) solution across devices used by staff and students. These tools will detect and mitigate malware infections in real-time, isolating compromised devices to prevent the spread of ransomware or other advanced threats. EDR solutions will address over 850 malicious URL requests and 79 known malicious IP addresses identified in the SLR.

4. **Cloud Security and Data Loss Prevention (DLP)**

As the district increasingly relies on SaaS-based applications, such as Microsoft Teams and Google Drive, the district will implement cloud security solutions to protect sensitive data. DLP tools will monitor cloud environments for unauthorized access or data leakage to safeguard sensitive information.

Sites Covered in the Pilot Project:

Note: substantially similar features, or their equivalents, are allowable

The project will cover all K-12 schools, administrative offices, and annexes that rely on the district's broadband network. These facilities have experienced increased network traffic due to the use of online learning tools and cloud-based applications. The proposed solutions will secure infrastructure across all these sites, ensuring uninterrupted access to educational resources while maintaining strict security controls.

Expected Outcomes:

Note: substantially similar features, or their equivalents, are allowable

By implementing the action plan with Cyber Storage NAS, Zerto CDP, Clear Pass NAC, and PAM, the district expects the following outcomes:

- ✓ Reduce Data Loss Risks: Cyber Storage NAS DLP and Zerto's disaster recovery tools will prevent unauthorized access to sensitive data, respond to file-based threats, and ensure fast recovery from incidents.
- ✓ A properly functioning NAC will prevent unauthorized users from accessing network resources by authenticating and authorizing users while monitoring and controlling network activity. It will also profile users and their devices, providing visibility into the devices connected to the network.
- ✓ Secure Privileged Access: PAM will reduce the risk of insider threats by managing and auditing access to sensitive systems.
- ✓ Mitigation of Malware and C2 Communications: EDR solutions reduce the risk of malware, ransomware, and Command and Control (C2) communications, thereby enhancing network security.
- ✓ This multi-layered cybersecurity strategy will significantly strengthen THE DISTRICT's defenses, ensuring its network remains resilient against external and internal threats while protecting critical educational resources.

O. Identity Protection and Authentication (Equivalent Solutions will be considered)

Note: substantially similar features, or their equivalents, are allowable

☑ Privileged Identity Management (PIM): PAM will enforce access controls for privileged accounts, ensuring that only authorized personnel can access critical systems and data.

☑ Multi-Factor Authentication (MFA): MFA will protect user identities and prevent unauthorized access to network resources.

☑ Web Content Controls and Email Security: Tools to prevent phishing, credential stuffing, and other email/web security threats.

Network Access Control (NAC): authenticate users and devices attempting to connect to the broadband network. It will identify authorized personnel, monitor device behavior, and ensure that only verified identities can access critical network components.

P. Monitoring, Detection, and Response

Note: substantially similar features, or their equivalents, are allowable

☑ Data Loss Prevention (DLP): Cyber Storage NAS DLP will monitor data movement and prevent unauthorized access or data leakage.

☑ Zerto for Continuous Data Protection and Disaster Recovery: Zerto ensures continuous data replication and rapid recovery in the event of a cyberattack.

These services will protect the district's network, devices, and data from a wide range of cyber threats while improving overall security posture and monitoring capabilities.

IV. PRODUCTS AND SERVICES REQUESTED

Note: substantially similar features, or their equivalents, are allowable

Privileged Access Management (PAM) 3-year licenses and support warranty if available.

Network Access Control Professional Services and 3-YR Support Renewal Cost Loss Prevention (Cyber Storage NAS) 3-Year

Vendors can bid all eligible items allowed by the Cyber Pilot. This is optional to the district.

These estimates reflect the cost of cybersecurity solutions that the St. Mary Parish School Board (SMPSB) will implement to enhance its network security, as well as the participant's share of both eligible and ineligible expenses.

The district looks forward to receiving input and proposals from highly qualified Cybersecurity experts to help protect our network.

V. VENDOR QUALIFICATIONS

All Vendors MUST have a Service Provider Identification Number (SPIN), an active Unique Entity Identifier (System for Award Management (SAM), an FCC registration

number (CORES), a current Form 498 or 499, and a current Service Provider Annual Certification (SPAC). All vendors must include a copy of these documents in their proposals. Vendors failing to include these documents may be disqualified from bidding on this project.

Vendors bidding on this project must have certifications in Cybersecurity and extensive experience in this area. Vendors must describe a minimum of five companies where cybersecurity work was performed and a description of the work. Please include the name of the Company, Contact Person, Telephone Number, and email address.

Please include copies of Cybersecurity certifications of personnel who will be working on this project.

Additionally, please provide the names of companies where security-cleared engineers from your company currently perform work, such as those in state or federal departments that require security clearances.

VI. MANDATORY PRE-BID MEETING

All vendors MUST attend a virtual pre-bid meeting to bid on this project. Vendors MUST log in to

https://teams.microsoft.com/l/meetup-join/19%3ameeting_YWE0YWZlY2YtYjQ5Mi00ZjkyLTg5YTgtMTE1MDY0MDRmM2Ez%40thread.v2/0?context=%7b%22Tid%22%3a%22e0aa8ef0-d7b2-46d6-8eed-313b0b170e97%22%2c%22Oid%22%3a%22bb6a073f-67e8-4911-b9c0-5c790a73faa4%22%7d

Meeting ID: 220 336 698 996 1
Passcode: hm7fu22W

on Monday May 12, 2025 by 10:00 AM (CST). The conference will open at 9:45 AM CST. No questions will be answered before the pre-bid meeting, and we expect vendors to be familiar with the FCC Cybersecurity Pilot Project.

VII. EVALUATION CRITERIA

The evaluation of each response will be based on its competence, compliance, format, and the criteria listed in the scoring sheet. Experience is scored based on the information provided in the proposal and the company's references. It is the service provider's responsibility to provide a convincing proposal that demonstrates their experience in Cybersecurity Services and Equipment.

Proposals that pass the preliminary screening and meet the mandatory requirements will be evaluated based on the criteria outlined below.

	Criteria	Maximum Score
1	Qualifications and Experience	20
2	Approach and Methodology	15
3	Proposed Technology/Solution and Perceived Value	15
4	Management Team Capabilities and Qualifications	20
5	Pricing	30
	Total	100

Discussions/Presentations

Written or oral discussions will be conducted with Vendors determined to be qualified to select the award. Written or oral discussions/presentations may be undertaken to clarify any or all components of the submitted proposal, thereby enhancing the district's understanding. The district reserves the right to conduct a Round 1 and 2 Evaluation. The same evaluation criteria will be used in both rounds.

VIII. PROPOSAL RESPONSE FORMAT AND DETAILS

Executive Summary.

The one- or two-page executive summary provides a brief description of the vendor's proposal. This summary should highlight the noteworthy features of the proposal. It must indicate any requirements that the Vendor cannot meet. The reader should be able to determine the essence of the plan by reading the executive summary. All pages must be numbered consecutively, and the name of the Vendor should appear in the header or footer.

Detailed Proposal

This section should constitute a sizable portion of the proposal and must contain the following:

The plan must include a comprehensive narrative of the Vendor's assessment of the work to be performed, their ability and approach, and the resources necessary to fulfill the requirements. It should demonstrate an understanding of the desired overall performance expectations. Indicate any options or alternatives proposed.

The Vendor must respond to each section and note the subsection. For ease of evaluation, the Vendor's response must immediately follow each item or specification (paragraph, sub-paragraph, etc.). For example, Section V describes the Vendor Qualifications. Vendors that disagree must indicate one of the options in the paragraph below. No response indicates acceptance and compliance.

Accept and comply - Follow this response with a brief, concise explanation that adequately details the Vendor's ability to meet the specified requirement unless the specification/requirement is clearly (unequivocally) a "yes or no," "can do or cannot do," "will or will not comply" type of specification, in which case "Accept and comply," without an accompanying explanation, will suffice.

Accept and comply with an exception – The vendor must clearly state the difference between the specification and the Vendor's ability to meet the specification's requirement(s).

Cannot comply - Follow this response with sufficient detail that explains why the specification cannot be met.

Exceptions and additions to the Standard Terms and Conditions must be submitted with the proposal response. Exceptions, additions, and service level agreements submitted after the specified receipt date and time will not be considered. The Vendor must submit a redline document identifying the proposed exceptions to the RFP terms and conditions with the proposal submission for review and evaluation purposes. The Vendor must provide the name, contact information, and access to the person(s) directly involved in legal negotiations of the terms and conditions in the proposal response.

Service providers uploading proposals to the electronic bidding site do not need to submit additional copies. However, if mailing or hand-delivering a proposal is required, one original and three duplicate copies of each proposal, plus one separate electronic copy in PDF format, must be included in the package. Electronic copies should be submitted on a clearly labeled flash drive. Only the PDF version is required if the proposal is uploaded to the bidding site. It is the vendor's responsibility to ensure that all documents are uploaded to the drive and are readable. All materials submitted in the proposal MUST be included in the electronic copy.

Receipt of Proposals

Responses for the entire RFP must be received at the address specified in this RFP on June 9, 2025, at 2:00 PM (CST) to be considered. Any bids received after the proposal opening time will be returned unopened.

IX. SPECIAL TERMS AND CONDITIONS

Suspensions and Debarments.

Persons and companies convicted of criminal violations or held civilly liable for individual acts arising from their participation in the Schools and Libraries (E-Rate) Program and other federal programs are subject to suspension and debarment from the program. The Federal Communications Commission (FCC) Suspension and Debarment regulations were announced in the Second Report and Order and Further Notice of Proposed Rulemaking (FCC 03-101 released April 30, 2003).

FCC rules provide that there are two stages to this process.

First, when the FCC becomes aware that a person or company has been convicted of a crime or found civilly liable for individual acts arising from their participation in the program, the FCC suspends that person or company from activities related to the program. The FCC issues a Public Notice of Suspension and Proposed Debarment. USAC maintains a list of individuals and companies that have been suspended, along with a link to the corresponding notice on the FCC's website. The suspension's announcement informs the suspended person or other interested parties that they have 30 days to oppose the proposed debarment.

The second stage of this process is the actual debarment. The FCC will, absent extraordinary circumstances, notice a decision to debar within 90 days of receiving any information from the person proposed for debarment. The notice will specify the duration of the debarment.

Contractual Period.

The district intends to award a thirty-six (36) month contract with two optional one-year extensions. The pilot program funding will end on June 30, 2028, unless otherwise extended by the FCC. However, the district may want to extend contracts and pay for continued services using alternative funding sources.

Delays in awarding beyond the anticipated starting date may change the contract period. If such a situation arises, an award may be made for a term of less than thirty-six (36) months.

YEAR 1				
YEAR 2				
YEAR 3				

X. SAMPLE OVERALL PROJECT PRICING SHEET

YEAR Recurring Services Equipment One-Time FEE TOTAL

The last section of the proposal should provide a detailed pricing sheet for all recurring services, equipment (including licenses), and one-time installation charges.

CERTIFICATION OF DEBARMENT-SUSPENSION

Certification Regarding Debarment, Suspension, Ineligibility, and Voluntary Exclusion - Lower Tier Covered Transactions

The regulations implementing Executive Order 12549, Debarment and Suspension, 7 CFR Part 3017, Section 3017, subpart c—Responsibilities of Participants, require this certification. The regulations were published in the Federal Register on November 26, 2003, on pages 66534-66566.

(BEFORE COMPLETING CERTIFICATION, READ ATTACHED INSTRUCTIONS)

(1) The prospective lower-tier participant certifies, by submission of this proposal, that neither it nor its principals are presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in this transaction by any Federal department or agency.

(3) Where the prospective lower-tier participant cannot certify any of the statements in this certification, such prospective participant shall attach an explanation to this proposal.

Cybersecurity Project

_____

Organization Name PR/Award Number or Project Name

_____

Name and Title of Authorized Representative

_____

Signature Date _____

The regulations implementing Executive Order 12549, Debarment and Suspension, 7 CFR Part 3017, Section 3017, subpart c—Responsibilities of Participants, require this certification. The regulations were published in the Federal Register on November 26, 2003, on pages 66534-66566.