# Cybersecurity Pilot Program
# Request for Proposal

## Madera Unified School District (BEN #144042)
### E-rate Form 470 Application

### Submission Deadline –August 6, 2025 at 5:00 PM, PST

The **Madera Unified School District** has been selected as a pilot for the Schools and Library Cybersecurity Pilot Program. Cybersecurity funds to help improve the security of our network.

**Madera Unified School District** is seeking proposals for Cybersecurity Monitoring, Detection, and Response and Identity Protection and Authentication services and equipment for its Cybersecurity Pilot Program application. The term of the contract shall be for a period of **3** years, renewable each year, beginning on the date the final pilot application is approved by USAC. The contract may be cancelled with thirty-day prior written notice. Depending on when the funding is awarded, a contract extension may be necessary to complete the full scope of work at each site.

The Offeror must submit a completed original proposal in accordance with the format provided in this solicitation to **Madera Unified School District** through e-mail **madera.erate@edtechnologyfunds.com** prior to 5:00 p.m. local time on the allowable contract date noted on the 470 application.

Questions and requests for clarification related to definition or interpretation of this RFP shall be submitted in writing via e-mail to **madera.erate@edtechnologyfunds.com**. No questions will be accepted via telephone and oral explanations or instructions shall not be considered binding on behalf of the Entity. If you have any other concerns or comments regarding this solicitation, please send an e-mail to the address listed above.

**Key Dates:**

The proposed project schedule for this RFP is as follows:

**RFP Published/Form 470 Posted:** .....**July 9, 2025**
**Service Provider Questions Due:** .....**July 24, 2025**
**Addendum with Replies to Service Provider Questions:** ..... **July 26, 2025**
**Service Provider Submissions Due:** .....**August 6, 2025**
**Service Start Date**: .....Upon Final Pilot Application Approved by USAC

**Service Provider Requirements:**

1. Service Provider must provide a valid SPIN at the time the bid is submitted, and the SPIN must be included in the response documentation.
2. Service Providers must have a current FCC Red Light Display System Status of Green.
3. Service Providers must demonstrate a minimum of 5 years of experience in K-12 education or city/county government markets.
4. Service providers must demonstrate a minimum of 5 years of experience in the Cybersecurity industry.
5. Service Providers must reference a minimum of (3) similar sized Cybersecurity projects Include contact name, contact email, contact phone number, total project dollar amount, project completion time, and a brief description of the project.
6. Service Providers must hold a valid and current manufacturers certification or equivalent for other manufacturers proposed. A copy of the certificate must be included in the proposal.
7. Service Providers must have Certified Network Resources. Service Providers may be required by the to provide proof certification.
8. Billed Entity Reimbursement or Service Provider method of invoicing may be elected The selected service provider must accept the selection made by the applicant.

**Project and Contract Requirements**

This project is dependent on partial funding from the Cybersecurity Pilot Program. All contracts entered into as a result of the posting of the Form 470/RFP will be contingent upon the approval of discounts from the Universal Services Administrative Company (USAC) and the **Madera Unified School District** acceptance of the funding award. No part of this contract will be valid or executed outside of Cybersecurity Pilot Program timelines and approvals unless authorized by the **Madera Unified School District**.

a. Appendix A Details the equipment required. Manufacturers with equivalent functionality can be quoted however all options must be compatible with existing infrastructure, systems, and applications.
b. All equipment and supporting components must be new. Used or refurbished items will not be accepted.
c. All components and associated labor not eligible for E-rate funding must be provided in a separate quote.
d. Estimated Discount is **90%**.
e. All pricing must include taxes, shipping/handling, and all other eligible fees.
f. Manufacturer's multi-year warranty for a period up to three years may be included in the cost of the component
g. The manufacturer's warranty must be valid and verifiable.
h. Prices must be held firm for the duration of the contract or until all work associated with the project(s) are complete (including any Universal Services Administrative Company (USAC) approved extensions).
i. Any implementation that is done prior to the funding award must be requested and approved in writing

j. Services covered by this contract cannot take place before the contract start date unless requested in writing.
k. Vendors must comply with all Local, State, and Federal contracting requirements applicable including bit not limited to:
    - Prevailing Wage
    - Insurance
l. Notice To Proceed:
    - This project is contingent on funding from the Cybersecurity Pilot Program. As such, the **Madera Unified School District** will not issue a Notice to Proceed until a copy of the approved Funding Commitment Decision Letter (FCDL) has been received from USAC and a Form 486 "Receipt of Service Conformation" has been filed. Contractor will not be permitted to commence work, unless otherwise directed, until a Notice to Proceed has been issued. **Madera Unified School District** will not be responsible for costs incurred by the Service Provider prior to receiving a Notice to Proceed.
m. Reservation of Rights:
    a. **Madera Unified School District** reserves the right to award all, none, or select portions of this bid to one or multiple Service Providers. **Madera Unified School District** reserves the right to negotiate terms and conditions of the RFP as necessary, to reject any or all proposals, to increase quantities, and to waive any irregularities or informalities in the RFP or in this process.

Bids Disqualification Criteria:

1. All “SPAM” and/or “Robotic” responses will not be considered valid bids and will be disqualified.
2. Only bids that supply a complete solution will be evaluated, and partial bids will be disqualified.
3. All bids that don’t include the requested services, term of services, and ineligible, will be disqualified.
4. Only one bid will be awarded for the Project, or Based on the project need, multiple vendors may be awarded

**Proposal Evaluation:**

It is anticipated that a contract will be made with the provider whose proposal is determined to be the most cost effective and in the overall best interest of **Madera Unified School District**. The main evaluation considerations are:
1) Price of Eligible Cybersecurity Service.
2)Price of Ineligible Cybersecurity Service.
3) Compatibly with Current Network, Systems, and/or Applications.
4) Prior Experience/Customer Satisfaction/Qualifications
5) Quality and Completeness of Proposed Solution

## APPENDIX A
## List of Equipment and scope of work required.

**Madera Unified School District** is seeking proposals from qualified vendors to obtain equipment and services for various infrastructure upgrades through the Cybersecurity Pilot Program For all items detailed below alternative manufactures and solutions can be proposed, but any alternatives must be compatible with the existing infrastructure systems and applications and must be cost effective. Additional items and quantities may be quoted as needed to complete the solution. All ineligible allocations on eligible components must be clearly included in your proposal. Components not eligible for Cybersecurity Pilot Program funding must be provided on a separate quote. The proposal must be listed by service type.

### XDR, SIEM, SOAR Project Requirements

Madera Unified is currently looking to expand its security posture by implementing a SOAR (Security Orchestration, Automation and Response) and SIEM (Security Information and Event Management) platform. At minimum, the District is looking for services that integrate with an XDR platform already in place (Palo Alto Cortex XDR), however bids may be submitted for a solution that incorporates all three services within a single platform (XDR, SOAR, SIEM). SOAR and SIEM service bids may be submitted on an individual basis, an all-in-one solution would be preferred. Bids for an XDR only solution will not be considered.

Solutions should have the following general features. This list is not exhaustive: Industry Standards will be required.

XDR Service requirements (If bidding on All-in-One solution)

- Behavior and hash based local analysis and threat prevention
- Exploit prevention mapped to MITRE ATT&CK framework
- Kernel-based exploit prevention
- Network inspection to prevent network based attacks
- Utilize advanced AI and Machine Learning for evolving threats
- Credential gathering protection
- Host Firewall Protections
- USB Device Controls
- Secure Remote Access
- Full CMD, Bash, Powershell and Python scripts or shell access
- Device Isolation while maintaining contact with Service
- Behavioral and Identity analytics
- Customized detections and IoCs
- Ability to ingest and act on data from District Infrastructure
- Ability to ingest threat intelligence feeds from third-party sources
- Incident management and investigation
- Asset and IP inventory

- Root cause analysis of alerts
- Querying of log data from all ingested sources
- Ability to coordinate on incidents with other team members
- Remote file detection and deletion
- Notification response for alerts and incidents
- Minimum 30 day hot storage for logs and incidents
- Notifications sent via multiple channels
- Role-based access control (RBAC)

SOAR Service requirements

- Ability to integrate with listed District Infrastructure
- Customizable automated playbooks(Workflows)
- Ability to run playbooks(Workflows) based on ingested events as well as on-demand
- Case management for events
- Ability to coordinate with other team members within case management
- Threat Intelligence integrations
- API based integrations available
- Automated data enrichment (e.g., WHOIS, VirusTotal, Sandboxing)
- Approval workflows for higher risk actions
- Role-based access control (RBAC)
- Notifications sent via multiple channels
- Cloud Hosted

SIEM Service requirements

- Support log ingestion from listed District Infrastructure
- Out-of-the-box correlation rules
- Flexible or automated log parsing
- Ability to create custom correlations
- Real-Time and scheduled alert creation
- Visual customizable dashboards
- Customizable reporting
- API based integrations available
- Utilize User & Entity Behavior Analytics
- Support for open detection sharing rules (e.g., Sigma, YARA, Snort)
- Notifications sent via multiple channels
- Role-based access control (RBAC)
- 90 day minimum “Hot” log retention
- 180 day minimum “Cold” log retention

All Services must be compatible with the following Infrastructure currently in use within the District

- 4,000 Estimated Traditional Endpoints
    - 250 Server OS Systems
        - Primarily Windows, Minority Linux
        - Primarily hosted on VSphere systems, some physical servers
    - 3000 Windows Endpoints
    - 750 MacOS Endpoints
- 30,000 ChromeOS (Chromebook) Devices
    - Not required for coverage
- 24,000 Estimated Total User Accounts
    - 20,500 Student Accounts
        - Various Grade Levels
    - 3,500 Staff Accounts
    - Accounts are both utilized within Microsoft Active Directory and Google Workspace
- 500 Network Switches
    - HP Aruba
- 2 Firewalls
    - Palo Alto
- 1300 Wireless Access Points
    - Ruckus
- Email hosted by Google Workspace
- On Premises Active Directory with integrations to Microsoft Azure
- Current Log ingestion is 180GB per day average.
    - Ingestion is not currently inclusive of all District Infrastructure
- Two On-Premises Security Staff

**Email Security and Automation Project Requirements**

Madera Unified is currently looking to expand its security posture by implementing an Email Security and Automation tool within its workflow. At minimum, the District is looking for a service that integrates with current infrastructure as well as planned simultaneous projects such as SIEM and SOAR platforms. Bids should be submitted with preference for securing staff accounts. Bids including student account coverage will also be considered.

Solutions should have the following general features. This list is not exhaustive: Industry Standards will be required.

- Real-time scanning for malicious attachments, URLs and Phishing attempts
- Detection of Business Email Compromise (BEC) attempts, spoofing and domain impersonation
- URL, Attachment and embedded content scanning
- Spam filtering and rules
- Customizable policies and feeds
- URL rewriting and time-of-click protection
- Sandboxing and real-time emulation of attachments in secure environment
- Support for automated actions based on events
- Integration with third-party threat intelligence feeds
- Reputation scoring for senders and domains
- Support for SPF, DKIM and DMARC policies and enforcement
- Ability to remove messages from inbox after delivery
- Prevent suspicious messages from being delivered and quarantine for review
- Search against messages for threat hunting purposes
- Logging of end-user interactions with a message
- Ability for end-user reporting of suspicious messages
- Integration with SIEM and SOAR platforms
- Open API integrations
- Role-based access control (RBAC)

Current District Infrastructure

- 24,000 Estimated Total User Accounts
    - 20,500 Student Accounts
        - Various Grade Levels
    - 3,500 Staff Accounts
- Email hosted by Google Workspace
    - Average of 200,000 Emails sent and received per day
- Two On-Premises Security Staff