

**E-Rate FY2026**

**CATEGORY 2  
INTERNAL CONNECTIONS  
SD-WAN Router/Gateway Equipment**

**RFP # 26-914**

**Questions and Answers #1**

**POSTED: December 1, 2025**

**Deadline for Submittal: January 6, 2026  
BEFORE 2:00 P.M.**

**ATTN: TECHNOLOGY SERVICES**

**Roseville City School District  
1050 Main Street  
Roseville, CA 95678**

1. If a vendor proposes utilizing existing, District-owned hardware for the Headend/District Office that is already fully installed and managed, but whose Threat Prevention Throughput specification is within a 10% tolerance (e.g., 9.2 Gbps) of the required minimum (10 Gbps), will this proposal be considered fully compliant, assuming the device fully meets or exceeds all other capacity metrics (e.g., sessions, new connections, firewall throughput)

**RESPONSE:** Yes. *The District will consider proposals that re-utilize existing, District-owned Headend/District Office hardware, provided that:*

- *The equipment is fully compatible with the proposed SD-WAN solution,*
- *It meets or exceeds all required capacity and performance metrics, and*
- *Any minor variance (such as a Threat Prevention Throughput rating within approximately 10% of the stated minimum) does not hinder the solution's ability to meet the District's operational, security, or performance objectives.*

*To ensure a consistent evaluation process, all proposals must include the full cost of the complete solution, **including** any equipment the vendor believes can be safely reused. Vendors may note where existing District equipment eliminates the need to procure specific items.*

2. If a vendor proposes utilizing existing, District-owned hardware for the Headend/District Office that is already fully installed and managed, but the support for this existing hardware extends to July 2027, with an End-of-Life (EoL) date of August 31, 2028. This EoL date is within the 36-month minimum EoL window required by the RFP (Section 6, Support and Warranty). Given that proposing the utilization of existing, District-owned equipment provides significant cost savings for this funding year, will the District grant an exception for existing infrastructure to be integrated into the SD-WAN solution under the condition that the proposed solution meets all other functional requirements and the vendor provides the full licensing and installation services required by this RFP?

**RESPONSE:** Yes. *As noted in the District's response to Question 1, the District is willing to re-utilize existing, District-owned equipment at the Headend/District Office, even if that hardware does not meet the RFP's preferred 36-month minimum manufacturer support window, provided that the proposed solution meets all functional, performance, and compatibility requirements of this RFP.*

*Because the existing hardware has manufacturer support through July 2027 and an End-of-Life (EoL) date in August 2028, the District will allow its integration into the proposed SD-WAN architecture under the following conditions:*

**Replacement Plan & Cost Transparency**

*Vendors must clearly identify and include:*

- *When the District's existing hardware will reach unsupported status, and*
- *The recommended replacement hardware, associated part numbers, and full costs required to maintain the solution past August 2028 compliance with this RFP over the contract term.*

**Inclusion of Full Project Cost**

*All proposals must still include the entire cost of the complete SD-WAN solution, including components the vendor believes can be safely reused. Vendors should explicitly note which items are not required due to existing District equipment.*

### *Support, Licensing, and Installation Requirements*

*Even when re-using District hardware, the vendor is still responsible for providing pricing of all required software licensing, support, configuration, installation, and integration services necessary for a successful implementation. Which includes:*

*- Any covering contract costs to cover existing equipment from August 2027 to August 2028*

*The District will consider the cost savings associated with utilizing existing infrastructure as part of its evaluation, provided that the proposed solution continues to meet all operational, security and performance requirements.*

### 3. WAN & Transport Questions

#### a. A. Current Circuit Info

- i. What WAN circuit types does each school currently have?

**RESPONSE:** *All sites currently have a MetroEthernet connection. Two of the sites in the District have a DIA Circuit to separate ISP's, as shown in Appendix C of this RFP. In addition, the District also has a secondary circuit, via our MetroEthernet to our County for services they offer.*

- ii. (MetroE, broadband, DIA, LTE, etc.)

**RESPONSE:** *MetroEthernet and DIA*

- iii. What are the bandwidth levels per site today?

**RESPONSE:** *For purposes of this RFP, all responses should use the drawing in Appendix C along with the information on Page 6 and 8 of the RFP. As mentioned, we have the following:*

*Site A: 17 Sites*

*Site B: 7 Sites*

*District Office: 1*

- iv. Are any sites scheduled for circuit upgrades or changes in the next 12–24 months?

**RESPONSE:** *Yes, depending on District funding, all sites are expected to be upgraded in the coming months with increased MetroEthernet speeds and/or DIA circuits as shown in Appendix C.*

- v. For sites using Metro Ethernet, what is the handoff interface type (10G SFP+, 1G copper, VLAN tagging, etc.)?

**RESPONSE:** *Currently all hand-off's are via 1G copper to the carrier where we have Untagged and Tagged VLANs on the port. The carrier then applies 802.1 QnQ*

#### b. B. Redundancy & Diversity

- i. Do you want dual Internet circuits at every site?

**RESPONSE:** *The District's current design plan is a MetroEthernet connection with a single DIA internet to each site.*

- ii. Do you require physically diverse carriers for resiliency (e.g., fiber + coax)?

**RESPONSE:** *Only diversity would be between Copper and Fiber handoff's between carriers.*

- iii. Is LTE/5G backup desirable for key campuses?  
**RESPONSE:** *The District has no desire for a LTE/5G enabled equipment, as any handoff from a carrier would be via a Copper or Fiber connection.*

4. Routing & Network Architecture

a. A. Internal Routing Model

- i. Are all sites currently running BGP back to the District Office?  
**RESPONSE:** *Yes, all sites are connected to our MetroEthernet where we have a BGP routing enabled at the core over a single AS number for all sites. Since all unrouted traffic is defaulted to the District Office, no other routing protocols are layered on top of the network. During this design plan we expect to need to overlay OSPF or other routing protocols to support the new SD-WAN backbone.*
- ii. Do any sites use static routing that needs to be modernized?  
**RESPONSE:** *Yes, but only at the District Office between our Core Routing Switch and our Firewall.*
- iii. Are you planning to keep your current BGP ASN architecture, or open to redesign?  
**RESPONSE:** *The District is open and expects that a re-design will be needed to accomplish the goals of the District and be able to support the SD-WAN overlay.*

b. B. VLAN & Core Switching

- i. Do the Aruba CX switches use consistent VLAN design across sites, or are there site-by-site variations?  
**RESPONSE:** *All sites, except the District Office and Student Services, have the same VLAN design across the entire district, with each site having a pre-defined subnet that is routed over the BGP.*

*The District Office and Student Services sites have additional VLANs that are not reflected at other sites, used mainly for network / virtual infrastructure controlling and signaling*

- ii. Do you require sub-interface designs or routed L3 handoffs?  
**RESPONSE:** *Not sure I fully understand the question*

*If this is in regards to InterVLAN routing within a site or Site-to-Site routing, then yes to both as the ultimate goal is to allow for each site to run independently wherever possible. The District prefers to not have all traffic sent to a single site unless required for a specific service.*

5. Internet Breakout & Security

a. Security Policies

- i. What security stack are you expecting at the edge?  
**RESPONSE:** *At this stage, the District has not finalized the handoff design with carriers, and we anticipate working collaboratively with both the awarded SD-WAN vendor and our transport providers to define the final specifications. Based on our current architecture and planning, the District expects the following:*

#### Carrier Handoff Expectations

- Direct Internet Access (DIA): The District anticipates DIA handoff occurring behind a carrier-supplied SNAT firewall.
- Metro Ethernet connections will continue to hand off via the existing configuration, as referenced in response 3.A.v within this Questions & Answers document.

#### District Traffic Flow Design - The District's current design approach is:

- Inbound internet traffic will only be accepted at one of two locations — the District Office or Westbrook.
- All other sites will be outbound-only, receiving return traffic from internet sessions they originate but no unsolicited inbound traffic.

The District is open to responder recommendations that improve the robustness, security posture, or operational efficiency of the proposed solution. If a vendor offers enhanced security capabilities (e.g., advanced threat protection, IDS/IPS, cloud-based filtering, sandboxing, encrypted traffic analysis), these may be included as optional line items, with:

- A description of the feature
- Any required subscriptions or licenses
- The functional benefit to the District

#### Minimum Required Security Capabilities - At a minimum, edge devices implemented as part of this SD-WAN solution must provide:

- Stateful Firewalling
- Application-Aware Controls
- Ability to intelligently identify, steer, or block traffic for both inbound (where allowed) and outbound sessions
- Threat Identification & Blocking
- Ability to detect and drop traffic associated with defined or known security threats (e.g., signatures, behavioral indicators, policy-defined rules)

These minimum criteria ensure that all participating vendors meet a baseline security posture, while also giving vendors room to differentiate their offerings where beneficial to the District.

- ii. (URL Filtering, Threat Prevention, DNS Security, WildFire, IPS/IDS)

**RESPONSE:** *We assumed this is related to the question above.*

- iii. Do different campuses need different content-filtering policies?

**RESPONSE:** *If this is related to student content-filtering (website content filtering) no. The District has content-filtering for student and staff devices and currently has no plans to change its student content-filtering during this work.*

*The existing content filter works via redundant inline appliances at the District Office and as installed agents on student devices. These agents will allow the devices to have the same filtering when on/off the District network.*

- iv. Do you require identity-based policy enforcement (User-ID / student vs staff)?

**RESPONSE:** *Currently we have this done by assigned IP Subnets that are applied during the device/user authentication to the network. At this time, we don't plan on modifying this during this re-design.*

6. SD-WAN Operations & Monitoring

a. Centralized Management

- i. Do you prefer cloud-hosted management (Strata Cloud Manager) or on-prem Panorama?

**RESPONSE:** *The District would prefer Cloud Based over On-Prem so that changes and diagnosing of the network can be done when not on the District Network or unable to connect back via the VPN.*

- ii. Do you require role-based access for school techs?

**RESPONSE:** *No, but would be preferred as we currently limit access to any networking infrastructure based on job responsibilities.*

7. HA / Failover Requirements

- i. Do you require every school to run HA pairs, or only high-impact sites?

**RESPONSE:** *Currently only the District Office has a HA pair of firewalls that is currently configured in an Active/Standby configuration.*

*For bidding purposes, this architecture should remain at the District Office.*

*All schools will not have HA pairs. The District will maintain a spare piece of equipment to be dispatched if and when needed. The District Office and one other site . The District maintains a spare equipment*

- ii. What failover behaviors do you expect (preemption, session sync, automatic failback)?

**RESPONSE:** *Active*

- iii. Are you okay with active/passive HA, or do you need active/active?

**RESPONSE:** *Active/Passive HA is acceptable*

- iv. Do you require bypass modes for power or link failure?

**RESPONSE:** *No. Bypass for link or power failure is not required*