All bid deadlines are 11:59pm Pacific Time the date of the bid deadline listed unless otherwise noted.

Midland ISD

IFCB Posted : Oct 30, 2026

Bid Deadline : Friday, Dec 11, 2026

Questions Due By : Sunday, Nov 8, 2026

Applicant Address : Midland, TX 79701

IFCB ID : 270003067

IFCB Requirements :

- Before the listed deadlines, all Questions and Bids must be submitted using the on-line IFCB system. Bids submitted before the bid deadline outside of this system will be disqualified. If the system is down before the deadline, please email your bid to info@crwconsulting.com or fax it to 918.445.0049. Bids or questions submitted in this fashion will be disqualified if the on-line system is active at the time of submission. The applicant reserves the right to request and obtain bids outside of the website system if the bid deadline has passed and zero or one bid is received (the intent for this is to follow USAC guidance on obtaining cost-effective bids).

- For all requested services and/or products listed on this IFCB: proposals that include generic/encyclopedic price lists will be considered non-responsive and will be disqualified. SPAM and/or robotic responses will not be considered valid bid responses and will be disqualified from consideration.

- Bidder must agree to participate in USF Program (AKA “E-rate”) for the corresponding funding year.

- Please include the correct Service Provider Identification Number (SPIN) on your bid.

- By submitting a bid, bidder certifies that the bidder does have a valid (non-red light status) SPIN for the E-rate program at the time of submission. Should the Applicant discover that the bidder is on red light status, or if the FCC classifies the bidder as on red-light status before work is performed and invoices are paid, the contract will be null and void and the applicant will have no payment obligations to the bidder.

- Bidder is expected to provide the lowest corresponding price per E-rate rules. See https://www.usac.org/e-rate/service-providers/step-2-responding-to-bids/lowest-corresponding-price/ for details.

- Contracts must not prohibit SPIN changes.

- Bidder must agree to provide the Applicant the choice of discount methods (SPI or BEAR).

- Bidder will be automatically disqualified if the District determines that the bidding company has offered any employee of the District any individual gift of more than $20 or gifts totaling more than $50 within a 12 month period.

- All contracts awarded will be contingent upon E-rate funding and final board approval. The applicant may choose to do all or part of the project upon funding notification.

- All applicable fees, surcharges, and taxes must be identified on the bid. E-rate rules require the applicants to evaluate the price of eligible goods and services that will be listed on the 471 application during the competitive bidding process. Fees and surcharges that apply but are not listed on the bid will be the responsibility of the bidding company, should their bid be awarded.

- If there is a request to purchase or lease new equipment, either Category Two or Category One, listed on this IFCB the applicant will accept bids for functionally equivalent equipment.

- E-rate rules require applicants to evaluate the cost of eligible goods and services, and to cost-allocate out the amount for ineligible services from their funding request. If your company will be bidding internet access service, please identify the amount to be cost-allocated out for the ineligible services – email service, web hosting, content filtering, or other bundled ineligible services.

- INTERNET ACCESS DISQUALIFICATION FACTOR: Bids submitted for services to an incorrect address will be disqualified.

- INTERNET ACCESS DISQUALIFICATION FACTOR: Your bid must identify the bandwidth you are proposing and associated price or your bid will be disqualified.

- INTERNET ACCESS DISQUALIFICATION FACTOR: Bids that do not include Dedicated Internet Access (guaranteed bandwidth, synchronous speeds) will be disqualified.

- INTERNET ACCESS DISQUALIFICATION FACTOR: Any and all installation charges must be identified on your bid. If you submit a bid indicating that installation charges may apply without listing those charges, we will consider your bid incomplete and disqualify your bid.

- DISQUALIFICATION FACTOR INTERNAL CONNECTIONS: The applicant will not accept bids from manufacturers of equipment deemed a national security threat by the Federal Communications Commission. The list of prohibited equipment is available here: https://www.fcc.gov/supplychain/coveredlist . Vendors that submit bids that includes these manufacturers will have their bid disqualified.

- DISQUALIFICATION FACTOR INTERNAL CONNECTIONS: Vendors must complete and include the C2 Cover Page with their bid. Bids received without the cover page will be disqualified.

- DISQUALIFICATION FACTOR INTERNAL CONNECTIONS: It will be the bidder’s responsibility to provide documentation about the compatibility requirements listed in this IFCB. Vendors that submit bids without documentation demonstrating the required compatibility listed in this IFCB will have their bids disqualified, unless that vendor has bid the preferred make/model number listed.

- DISQUALIFICATION FACTOR INTERNAL CONNECTIONS: Applicant will not accept bids for refurbished equipment. Any bids containing refurbished equipment will be disqualified.

- DISQUALIFICATION FACTOR INTERNAL CONNECTIONS: Service providers are required to bid an entire Project A, Project B, Project C and/or Project D. Bids for individual components, or bids that do not include all of the requested items for the project will be disqualified.

- DISQUALIFICATION FACTOR BMIC: Service providers are required to bid the entire maintenance project. Bids for individual components of the project will be disqualified.

- DISQUALIFICATION FACTOR BMIC: Vendors must complete and include the C2 Cover Page with their bid. Bids received without the cover page will be disqualified.

- DISQUALIFICATION FACTOR BMIC: Maintenance bids listing only an hourly rate and not a monthly or annual total will be disqualified. Vendors quoting an hourly rate are required to also a) confirm that you have the ability/expertise to maintain all of the equipment listed and b) propose a number of hours at a particular rate monthly to properly maintain the entire list of equipment. Bids that contain only hourly rates, without confirmation that the company can service the list of equipment, or without a monthly total will be disqualified.

Services and Equipment Requested :

Category One:

Internet Access – 20 GB bandwidth, this circuit comes into the district at (Admin) 615 W. Missouri Ave, Midland TX 79701.

After the initial term, or after any voluntary renewal terms are executed, the Vendor must offer up to 12 months of a month-to-month service if the Applicant decides to transition to a new service provider. Vendor must list that monthly cost as part of their proposal.

E-rate rules require applicants to evaluate the cost of eligible goods and services, and to cost-allocate out the amount for ineligible services from their funding request. If your company will be bidding internet access service, please identify the amount to be cost-allocated out for the ineligible services – email service, web hosting, content filtering, or other bundled ineligible services.

INTERNET ACCESS DISQUALIFICATION FACTOR: Bids submitted for services to an incorrect address will be disqualified.

INTERNET ACCESS DISQUALIFICATION FACTOR: Your bid must identify the bandwidth you are proposing and associated price or your bid will be disqualified.

INTERNET ACCESS DISQUALIFICATION FACTOR: Bids that do not include Dedicated Internet Access (guaranteed bandwidth, synchronous speeds) will be disqualified.

INTERNET ACCESS DISQUALIFICATION FACTOR: Any and all installation charges must be identified on your bid. If you submit a bid indicating that installation charges may apply without listing those charges, we will consider your bid incomplete and disqualify your bid.

Internet Access – 20 GB bandwidth, this circuit comes into the district at (Legacy HS) 3500 Neely Ave, Midland TX 79707.

After the initial term, or after any voluntary renewal terms are executed, the Vendor must offer up to 12 months of a month-to-month service if the Applicant decides to transition to a new service provider. Vendor must list that monthly cost as part of their proposal.

E-rate rules require applicants to evaluate the cost of eligible goods and services, and to cost-allocate out the amount for ineligible services from their funding request. If your company will be bidding internet access service, please identify the amount to be cost-allocated out for the ineligible services – email service, web hosting, content filtering, or other bundled ineligible services.

INTERNET ACCESS DISQUALIFICATION FACTOR: Bids submitted for services to an incorrect address will be disqualified.

INTERNET ACCESS DISQUALIFICATION FACTOR: Your bid must identify the bandwidth you are proposing and associated price or your bid will be disqualified.

INTERNET ACCESS DISQUALIFICATION FACTOR: Bids that do not include Dedicated Internet Access (guaranteed bandwidth, synchronous speeds) will be disqualified.

INTERNET ACCESS DISQUALIFICATION FACTOR: Any and all installation charges must be identified on your bid. If you submit a bid indicating that installation charges may apply without listing those charges, we will consider your bid incomplete and disqualify your bid.

Category Two:

VOLUNTARY SITE VISIT

Vendors wishing to bid on C2 can attend a voluntary site visit between the dates of November 2nd 2026 through November 6th, 2026. Vendors should RSVP to James Kenimer at james.kenimer@midlandisd.net to set up a time for a site visit on November 2nd 2026 through November 6th, 2026. Please email with at least 24 hour notice. THIS EMAIL IS TO RSVP ONLY. ALL QUESTIONS AND BIDS MUST STILL BE SUBMITTED VIA THE IFCB. BIDS NOT SUBMITTED VIA THE IFCB WILL BE DISQUALIFIED.

INTERNAL CONNECTIONS

Midland ISD is modernizing its core network infrastructure to support current educational delivery and operational needs. The following projects include deploying managed switches and wireless access points across school facilities and replacing firewalls to maintain the current security posture and scalability.

The existing infrastructure consists of aging equipment nearing the end of its life, which limits bandwidth, management capabilities, and security controls.

The new architecture will provide - Improved connectivity: Modern switching and wireless technology support increased device density and bandwidth requirements for classroom technology and online learning platforms.

Centralized management: Aruba Central and Cisco DNA licensing enable unified configuration, visibility, and troubleshooting across all network assets.
Enhanced security: firewall with advanced threat prevention, URL filtering, and DNS security protects student and staff data.

Operational efficiency: Modern equipment reduces support overhead, enabling IT staff to focus on instructional technology and security.
Replacing aged and non-standard cables and connections.

Installation and configuration services ensure minimal disruption to educational operations through structured deployment and knowledge transfer. This project directly supports the district's technology integration goals and improves the reliability of systems that students and staff depend on daily.

IC PROJECT A – WAPS

Full installation of hardware, and replacement of existing APs in ceiling locations across all buildings, including outdoor bracket installation and external AP deployment where required. Removal and collection of old Aps. Printed hostname Labels and Inventory stickers, and post-installation documentation to include inventory, on the devices prior to installation.

Type of Equipment	Quantity Vendor Should Bid	Preferred Make/Manufacturer
Cabling	500	Slim CAT 6 patch cables
Wireless Access Points	440	Aruba AP-635 no ceiling mounts with 5-year license
Wireless Access Points	25	Aruba AP-675 with bracket with 5-year license

COMPATIBILITY REQUIREMENT:
All Wireless Access Points must be compatible with Aruba Central management and our existing Central group configuration and site architecture.

DISQUALIFICATION FACTOR INTERNAL CONNECTIONS: It will be the bidder’s responsibility to provide documentation about the compatibility requirements listed in this IFCB. Vendors that submit bids without documentation demonstrating the required compatibility listed in this IFCB will have their bids disqualified, unless that vendor has bid the preferred make/model number listed.

IC PROJECT B – SWITCHES
Installation and configuration at replacement locations using existing power distribution. Include fiber connection Jumpers, modules, and network jumpers in the bid. Integration with existing network architecture. Include Stacking cables and power stacking capabilities.

Type of Equipment	Quantity Vendor Should Bid	Preferred Make/Manufacturer
Cabling	50	10 GB DAC cables, 1 meter
Cabling	3000	Slim CAT 6 patch cables
Cabling	60	Aqua MM Fiber Patch LC-LC, 3 meter
Antennas, Connectors and Related Components	30	10 G MM SFP
Switches	74	Cisco 9300-48UN with 5 year licensing
Switches	6	Cisco 9200L-48P-4X w 5 year licensing

COMPATIBILITY REQUIREMENT:
All switches must support our current Cisco-based network ecosystem and integrate with our existing VoIP infrastructure and network management protocols. Include Stacking cables and power stacking capabilities.

DISQUALIFICATION FACTOR INTERNAL CONNECTIONS: It will be the bidder’s responsibility to provide documentation about the compatibility requirements listed in this IFCB. Vendors that submit bids without documentation demonstrating the required compatibility listed in this IFCB will have their bids disqualified, unless that vendor has bid the preferred make/model number listed.

IC PROJECT C – FIREWALL
Installation, configuration, and migration of existing configuration and security policies. Include BGP, VPN, IPSEC, and best-practice configuration. Includes Pro service for initial setup and operational handoff.

Firewall must support policy migration from existing configuration rule sets. And be able to achieve a minimum throughput of 25 Gbps when threat prevention and IPSec are enabled.

Type of Equipment	Quantity Vendor Should Bid	Preferred Make/Manufacturer
Firewall Service and components	2	Palo Alto PA-5430 - Pro service and Education SKU with a 5-year term (60 months). Subscription bundles include, but are not limited to, Advanced Threat Prevention, Advanced URL Filtering, Advanced DNS Security, Advanced SD-WAN, and Device Security. Include training or education for 2 staff members, either virtual, self-paced, or education credits

NOTE: We are requesting firewall licenses on this IFCB, which sometimes may be categorized as BMIC or MIBS by USAC (the BMIC and MIBS boxes on the 470 have been checked to cover this scenario).

COMPATIBILITY REQUIREMENT:
Firewall must support policy migration from existing configuration rule sets.

DISQUALIFICATION FACTOR INTERNAL CONNECTIONS: It will be the bidder’s responsibility to provide documentation about the compatibility requirements listed in this IFCB. Vendors that submit bids without documentation demonstrating the required compatibility listed in this IFCB will have their bids disqualified, unless that vendor has bid the preferred make/model number listed.

IC PROJECT D – WAP LICENSING

Type of Equipment	Quantity Vendor Should Bid	Preferred Make/Manufacturer
Wireless Access Point Licensing	1776	1 year Aruba Central for existing WAPs

COMPATIBILITY REQUIREMENT:
Licensing must be compatible with Aruba Central management and our existing Central group configuration and site architecture.

DISQUALIFICATION FACTOR INTERNAL CONNECTIONS: The applicant will not accept bids from manufacturers of equipment deemed a national security threat by the Federal Communications Commission. The list of prohibited equipment is available here: https://www.fcc.gov/supplychain/coveredlist . Vendors that submit bids that includes these manufacturers will have their bid disqualified.

DISQUALIFICATION FACTOR INTERNAL CONNECTIONS: Vendors must complete and include the C2 Cover Page with their bid. Bids received without the cover page will be disqualified.

DISQUALIFICATION FACTOR INTERNAL CONNECTIONS: It will be the bidder’s responsibility to provide documentation about the compatibility requirements listed in this IFCB. Vendors that submit bids without documentation demonstrating the required compatibility listed in this IFCB will have their bids disqualified, unless that vendor has bid the preferred make/model number listed.

DISQUALIFICATION FACTOR INTERNAL CONNECTIONS: Applicant will not accept bids for refurbished equipment. Any bids containing refurbished equipment will be disqualified.

DISQUALIFICATION FACTOR INTERNAL CONNECTIONS: Service providers are required to bid an entire Project A, Project B, Project C and/or Project D. Bids for individual components, or bids that do not include all of the requested items for the project will be disqualified.

BASIC MAINTENANCE OF INTERNAL CONNECTIONS:
The district would like a manufacturer’s support contract for these items:

Type of Equipment	Quantity Vendor Should Bid	Preferred Make/Manufacturer
Firewall Service and components	2	Palo Alto PA-5430 - Pro service and Education SKU with a 5-year term (60 months). Subscription bundles include, but are not limited to, Advanced Threat Prevention, Advanced URL Filtering, Advanced DNS Security, Advanced SD-WAN, and Device Security. Include training or education for 2 staff members, either virtual, self-paced, or education credits

DISQUALIFICATION FACTOR BMIC: Service providers are required to bid the entire maintenance project. Bids for individual components of the project will be disqualified.

DISQUALIFICATION FACTOR BMIC: Vendors must complete and include the C2 Cover Page with their bid. Bids received without the cover page will be disqualified.

DISQUALIFICATION FACTOR BMIC: Maintenance bids listing only an hourly rate and not a monthly or annual total will be disqualified. Vendors quoting an hourly rate are required to also a) confirm that you have the ability/expertise to maintain all of the equipment listed and b) propose a number of hours at a particular rate monthly to properly maintain the entire list of equipment. Bids that contain only hourly rates, without confirmation that the company can service the list of equipment, or without a monthly total will be disqualified.

There is an additional document associated with this IFCB. Please click the buttons to download the document.

2026_C2_Bidding_Instructions71.pdf
MIDLAND_C2_COVER_PAGE6.pdf

Questions Received with Applicant Answers (Ask Questions?)

Related to IC Project C - FIREWALL: • Should transceivers be included within the scope of this proposal? If transceivers are required, please provide the specific transceiver types (e.g., 10G-SR, 10G-LR, 40G/100G optics), connector types, and the required quantities. • Please clarify the intended use case for the two firewalls. Is the secondary hardware required to function in an HA configuration identical to the primary appliance? Or is the requirement for a dedicated smaller form factor appliance for VPN traffic? • What is the estimated concurrent VPN user count and aggregate throughput requirements for VPN traffic? • Is mobile device or Linux support required for VPN? Are Host Information Profile (HIP) checks required?

Answer:

1. Transceivers
Yes, include transceivers in the proposal. Required per appliance:

[8] x 10G SFP+ SR, LC duplex, multimode (internal/core uplinks)
[4] x [40G QSFP+], [LC], [MM] (core or WAN handoff)

Proposed optics must be manufacturer-branded or manufacturer-certified compatible with the proposed appliance.

2. Use case for the two firewalls
The two appliances replace our existing primary data center and disaster recovery firewalls. Each is a full-function perimeter firewall at a separate site, not an HA pair at one location, nor a dedicated VPN appliance. Both units should be the same model with identical capabilities, so either site can carry the full district traffic, including remote-access VPN, if the other is down.

3. Concurrent VPN users and throughput

Estimated concurrent remote access users: [normal ~3, peak ~25]
Aggregate VPN throughput: [300 Mbps] sustained
Site-to-site IPsec tunnels: [4], including vendor tunnels (e.g., SIS database connectivity)
Firewall/threat protection throughput sized for [25 Gbps] per internet circuit(s) with [growth headroom 3 to 5 years]

4. VPN client platforms

Clients: Windows and macOS required. iOS/Android not required. Linux is not required.
Authentication: SAML 2.0 integration with Google Workspace is required. The current deployment uses an IPsec client VPN with SAML.
Posture checks (HIP or equivalent): [Not required].

Q&As from the walkthrough are below.

Answer:

Question: How should old APs be handled when removed? Is t
agging and bagging
required?
Response: T
he vendor
s
hould
remove all existing APs and
store
each unit at the time of removal. For each removed AP, the vendor will record the following on a spreadsheet provided to MISD at project completion:
• Building
• Room number or location
• MAC address
• Serial number
• Model
Removed APs will be boxed by building, with each box labeled with the building name and the count of APs inside. Removed mounting hardware will be bagged with its AP or boxed separately by building.
Boxes will be staged at
the Central admin building
for MISD retrieval. Vendor is not responsible for disposal of removed equipment.

Question: Does MISD want the cabling electronically identified?
Response: Yes. Vendor will test each AP cable run with a cable tester
to identify the cable type
and include the results in the post-installation documentation.
For each AP location, documentation will include:
• Building and room number
.

• AP
hostname.

• Patch panel and port number
.

• Cable category identified by testing (Cat5e, Cat6, or Cat6a)
.

• Cable length
.

Question: Should existing patch cables be
replaced with
slim Cat6 cables?
Response: Yes. The bid should include replacement of the closet-side patch cable for every AP being replaced, in the MDF or IDF serving that AP.
Vendor s
hould
:
• Remove the existing patch cable between the patch panel and the switch port for each AP
.

• Install a new slim Cat6 patch cable at the correct length for a clean run
.

• Match the color standard used for AP connections, [B
lue

]
• Maintain the existing patch panel to switch port mapping
.

• Dress and route cables through existing cable management
.

• Box removed patch cables for MISD retrieval with the removed APs
.

The 500 slim patch cables in the bid include spares. Unused cables will be turned over to MISD at project completion.

Question: How high are the AP locations?
Response: Classroom and office AP locations are mounted at approximately 10 feet and are reachable with a standard ladder.
Large spaces such as gymnasiums, cafeterias, auditoriums, and libraries may have AP locations at a height of [10 to 20] feet.
Outdoor AP locations at elementary campuses are mounted at approximately 10 to 16 feet. Outdoor locations at secondary campuses are 10 to 20 feet.
Vendor is responsible for providing all ladders, and safety equipment needed to complete the installation
.

Question: Are ceiling mounts required?
Response: MISD will reuse existing ceiling mounts for indoor AP-635 locations. Vendors will verify existing mounts are compatible with the AP-635 and report any locations where they are not, including hard ceiling or wall-mounted locations, before installation.
Outdoor AP-675 locations require new mounting hardware. Vendors should include the Aruba outdoor mount kit for each AP-675, suitable for wall mounting, along with any anchors, fasteners, and weatherproofing needed for a complete installation.

Question: Are there any new AP locations or new cable runs required?
Response: This project is a one-for-one replacement. Each new AP will be installed at the location of an existing AP, both indoor and outdoor. No new AP locations or new cable runs are included in this scope.
Vendors will reuse existing horizontal cabling. Any drop that fails testing or cannot support the AP uplink will be reported to MISD, as described in the cable testing response. Any repair or new cabling will be handled as a separate change order with MISD approval before work is performed.

Q&As from a walkthrough are below.

Answer:

Question 1: What make, model, quantity
,
and software version are the firewalls being replaced?
Response: Two Fortinet FortiGate 2200E appliances, one at the primary data center and one at the DR site, running FortiOS 7.4.x. Serial numbers will not be released. Current FortiCare/FortiGuard support ends
11-2027.

Question 2: Roughly how many security policy rules and NAT rules will need to be migrated? Are the VPN figures in the posted Q&A (4 IPsec tunnels, about 25 peak remote users) still current?
Response: About [
117
] security policies, [
68
] NAT/VIP rules, and [
5827
] address objects and groups per firewall. This includes large FQDN and IP-based blocklists for state-mandated prohibited technology. The VPN figures already posted [are still current
: 4 TUNNELS, 25 VPN USERS
]. Remote access uses IPsec client VPN with Google SAML authentication at both sites.

Question 3: Does the district use Panorama, Strata Cloud Manager, or another firewall manager today? Should bids include management licensing, or will existing management stay in place?
Response: The district does not use a centralized firewall manager today
; we use FortiManager on each firewall
. Bids [should not] include centralized management licensing for the proposed platform, priced as a separate line item.

Question 4: Can you confirm the two install sites (Admin at 615 W. Missouri and Legacy HS at 3500 Neely, or others)? Is an on-site cutover required, or is remote assistance acceptable? Are there required maintenance windows or after-hours rules?
Response: Install sites are [primary data center at
615 W. Missouri] and [DR site at 3500 Neely
]. On-site installation and cutover are required. Cutover must occur during district-approved maintenance windows, typically [weekends / after 6 PM on weekdays], and is scheduled with district IT at least [14] business days in advance.

Question 5: Does “Pro service” for initial setup and handoff mean a Palo Alto Professional Services engagement, installation and migration by the vendor, or both?
Response: This means vendor-performed installation, configuration, policy migration from FortiGate, cutover support, and documented handoff to district staff. Manufacturer professional services may be included if the vendor uses them to deliver that scope, but are not required on their own.

Question 6: The BMIC section repeats the same PA-5430 5-year bundle as Project C. If we bid Project C, should we also complete the BMIC line, and how should the 5-year subscriptions be split so nothing is counted twice?
Response: Price the 5-year subscription bundle once, under Project C. Bidders should not repeat the same subscriptions in the BMIC section. If BMIC pricing is provided, it should cover only basic maintenance services that are not already included
in the Project C bundle.

Question 7: When do the current firewall subscriptions expire, and what start date are you targeting for the new 60-month term?
Response: Current subscriptions expire
[11-2027
]. The district is targeting a [July 1, 2027] start for the new 60-month term, aligned with the E-Rate funding year.

Q&As from a walkthrough are below.

Answer:

Question: What power supply configuration is required?
Response: All switches require dual, hot-swappable power supplies. Power supplies must be sized to deliver full PoE+ (30W) on all 48 ports simultaneously, with the switch running at full load
.

• Cisco 9300-48UN: dual 1100W AC power supplies (PWR-C1-1100WAC-P or equivalent)
• Cisco 9200L-48P-4X: dual 1000W AC power supplies (PWR-C5-1KWAC or equivalent)
Include StackPower cables for all 9300 stacks. Vendors will provide power cords compatible with the existing rack power distribution in each closet.

Question: Should existing patch cables be replaced with the slim Cat6 cables?
Response: Yes. T
he vendor
will replace all patch cables on the switches being replaced with the slim Cat6 patch cables included in the bid.

Vendor s
hould
:
• Document each existing patch panel to switch port connection before removal
• Re-patch e
ach
port to the new switch, preserving existing port mapping unless MISD directs otherwise
• Follow existing color standards for AP, phone, and data connections
{blue}

• Dress and route cables through existing cable management
• Box removed patch cables for MISD retrieval
Unused cables will be turned over to MISD at project completion.

Question: What configuration work is required?
Response:
MISD
will provide configuration
guidance
for each r
eplacement, and the vendor will configure
as either a one-for-one swap or a stack, as designated by MISD per closet.

Vendor s
hould
:
• Pull the running configuration from each existing switch and migrate it to the new switch or stack, including VLANs, voice VLAN, trunks, port settings, QoS, SNMP, AAA, NTP, syslog, and management settings
• Convert per-switch port configurations to stack member numbering where switches are being stacked
• Submit migrated configurations to MISD for review and approval before cutover
• Perform cutover during MISD-approved maintenance windows
• Verify after cutover that uplinks, phones, APs, and end devices are online and match pre-cutover status
• Provide final configurations and a port map for each closet at project completion
MISD will provide a closet list identifying which locations are one-for-one swaps and which are stacked, along with stack member counts.

Question: Should stacking and power stacking cables be included?
Response: Yes. Vendor will include all stacking components required for the designated stack layout:
• Cisco 9300: StackWise-480 data stacking cables and StackPower cables for every stack member, in lengths suitable for the rack layout, including the cable closing the ring
• Cisco 9200L : StackWise-80 stack kit for each stacked 9200L. The 9200L does not support StackPower, so power stacking applies

to the 9300 only.

Related to the LAN Switching under IC Project B: • Will MISD require any uplink modules with the C9300? If so what speed? Without them it doesn't have any SFP ports. • Will MISD require stacking cables? If yes, please specify length (options are 50CM, 1M and 3M) and how many of each. • Will MISD require any stack kits for the C9200L's? If yes, please specify the length of stack cable (options are 50CM, 1M and 3M) and how many of each. • How many power supplies should be included with each switch on both the 9300 and 9200L's? • If dual power supplies are required for the C9300's, will power stacking cables be required? If so, please specify how many and what length (options are 30CM and 150CM.) • Kindly specify which level of DNA licensing is required for each model switch. Options are DNA-Advantage or DNA-Essentials. • Kindly confirm that the "EDU" version of these switches if available, would be acceptable. EDU designation includes 3YR of TAC access (phone support only.) With that, we would ask MISD to confirm that no additional uplifted support level or term duration would be required for SMARTnet on top of what the EDU SKU offers. Example: "C9300-48UN-EDU" and "C9200L-48P-4X-EDU" • Kindly confirm the C9200 model should be the C9200-48P-4X fixed uplink version and not the modular version "C9200-48PXG." Related to the WAPs under IC Project A - • Where will the Aruba 675's be mounted? Asking to determine which mounting bracket is needed i.e Pole mount, Wall mount, etc. See options below: • R9H97A – HPE Aruba Networking AP-OUT-MNT-V1A Outdoor AP long-arm pole/wall mounting bracket • JW053A – HPE Aruba Networking AP-270-MNT-V2, Outdoor AP short-arm pole/wall mounting bracket • JW054A – HPE Aruba Networking AP-270-MNT-H1, Outdoor AP hanging, one-way tilt pole/wall mounting bracket • JW055A – HPE Aruba Networking AP-270-MNT-H2, Outdoor AP flush wall mounting bracket • R6W11A – HPE Aruba Networking AP-270-MNT-H3, Outdoor AP hanging, dual-tilt pole/wall mounting bracket

Answer:

1. Uplink modules for the C9300
Response: Yes. Bid one C9300-NM-8X (8 x 10G SFP+) network module per C9300-48UN, 74 total. All switches will be deployed in stacks. Final uplink placement will be determined after award, and any unused modules will be retained by MISD.

2. 9300 stacking cables
Response: Yes. Bid one StackWise-480 stacking cable per C9300-48UN, 74 total, shorter length. All switches will be deployed in stacks. With 10 x 3-foot stacking cables to finish the stack loop. Final stack layout will be determined after award, and any cables not used in a stack will be retained by MISD.

3. 9200L stack kits
Response: Yes. Bid one C9200L-STACK-KIT per C9200L-48P-4X, 6 total, with one short stacking cable per switch. Final stack layout will be determined after award.

4. Power supplies per switch
Response: Two power supplies per switch for both models. C9300-48UN: dual PWR-C1-1100WAC-P. C9200L-48P-4X: dual PWR-C5-1KWAC. This is for full PoE power.

5. StackPower cables
Response: Yes. Bid one StackPower cable per C9300-48UN, 74 total, short length. With 10 x 3-foot stacking cables to finish the stack loop. The final power stack layout will be determined after award, and any unused cables will be retained by MISD.

6. DNA licensing level
Response: DNA-Advantage for both the C9300-48UN and the C9200L-48P-4X. MISD understands DNA-Advantage is included with the EDU SKU for the license term.

7. EDU SKUs
Response: Confirmed. EDU SKUs are acceptable. No additional SmartNet or uplifted support is required in this bid. MISD will identify and procure SmartNet coverage for the 9300 and 9200L separately each year.

8. C9200 model
Response: Confirmed. The required model is the C9200L-48P-4X with fixed 4 x 10G uplinks. Do not bid the modular C9200 or the C9200-48PXG.

IC Project A: WAPs

9. AP-675 mounting brackets
Response: The indoor ceiling-mount information has been addressed in a previous response. The 25 AP-675s are one-for-one replacements at existing outdoor AP locations. Vendors should include one JW053A (AP-270-MNT-V2, wall bracket) per AP-675, 25 total.

Related to Firewall IC Project C - Existing Environment and Architecture 1. What are the manufacturer, model, software version, and quantity of the existing firewalls being replaced? 2. Will the two new firewalls be deployed as a High Availability (HA) pair (active/passive or active/active) or as independent firewalls? At which location(s) will they be installed? 3. Can the District provide a high-level network diagram showing the existing firewalls, internet connections, core network, and relevant routing topology? 4. Are the existing firewalls managed locally or through a centralized management platform? Is centralized management required for the new firewalls? Firewall Configuration and Migration 5. Is the expected migration a like-for-like replacement of existing configurations and security policies, or does the District require policy redesign, optimization, or implementation of new capabilities? 6. Approximately how many Access Control Lists (ACLs), security policy rules, NAT rules, security zones, interfaces, and virtual routers are currently configured and need to be migrated? 7. How many BGP peers, site-to-site IPsec VPN tunnels, and remote-access VPN users must be migrated? Are changes to routing or VPN architecture expected? 8. Are any additional capabilities currently deployed, such as SSL/TLS decryption, User-ID, Remote Access VPN, or third-party authentication integrations, that must be migrated? Security Feature Implementation 9. For the requested security subscriptions, does the District expect license activation and baseline configuration, migration of existing security features, or full implementation of new capabilities? 10. Advanced Threat Prevention: Are there existing customized threat prevention profiles, exceptions, or specific security requirements that must be migrated or incorporated into the new deployment? 11. Advanced URL Filtering: Are there existing URL filtering policies, custom categories, or exceptions to migrate? Are any new filtering requirements expected? 12. Advanced DNS Security: Are there custom DNS security requirements, exceptions, or third-party DNS integrations that must be maintained or implemented? 13. Advanced SD-WAN: Is SD-WAN functionality currently deployed? Does the District require subscription activation only or a complete SD-WAN implementation? If implementation is required, how many sites and WAN circuits are involved? 14. Device Security: Does the District require basic licensing and onboarding or full device discovery, classification, risk monitoring, and device-based security policies? Approximately how many devices or network segments are in scope? 15. SSL/TLS Decryption: Does the District require migration of existing decryption policies or implementation of new decryption capabilities, including certificates and exceptions? 16. GlobalProtect / User-ID: Does the District require migration or new implementation of remote-access VPN, identity integration, authentication, or endpoint posture (HIP) policies? 17. Logging and Monitoring: What centralized management, logging, SIEM, or monitoring integrations must be maintained or newly implemented? Implementation and Cutover 18. Will the District provide rack space, power, cabling, transceivers, and physical connections, or should the vendor include onsite installation and connectivity services? 19. Can configuration, migration, and testing be performed remotely, or is onsite engineering required? 20. Are after-hours or weekend cutover windows required? Does the District expect a single cutover or multiple phased migrations? 21. Are there any District-specific acceptance criteria, critical applications, or operational requirements that require additional validation beyond standard firewall migration and failover testing? 22. The RFP specifies a minimum of 25 Gbps throughput with Threat Prevention and IPsec enabled. What are the expected peak traffic throughput, concurrent VPN usage, and SSL/TLS decryption requirements? Project Delivery and Knowledge Transfer 23. Will District IT personnel be available to assist with configuration access, network coordination, change management, and application testing? 24. Is there a required project completion date or preferred implementation schedule? 25. Beyond standard implementation documentation and operational handoff, does the District require any customized administrator training, operational runbooks, or additional knowledge transfer services?

Answer:

Existing Environment and Architecture

1. Manufacturer, model, software version, and quantity of existing firewalls
Response: Two Fortinet FortiGate 2200E firewalls, one at the primary data center and one at the disaster recovery site. Both run FortiOS 7.4.13.

2. HA pair or independent firewalls, and locations
Response: The two new firewalls will be deployed as independent firewalls, one at the primary data center and one at the disaster recovery site, replacing the existing FortiGates at each location. They are not an HA pair. Each unit must be capable of carrying the full district traffic, including remote-access VPN traffic, if the other site is unavailable.

3. High-level network diagram
Response: MISD will provide a high-level diagram showing the existing firewalls, internet connections, core network, and routing topology to [the awarded vendor (s) who request it and agree to the district agreement]. Detailed network diagrams will not be posted publicly.

4. Local or centralized management
Response: Existing firewalls are [managed locally on each appliance]. Logging is sent to [Fortinet cloud]. The firewalls also integrate with NetBrain via API for monitoring. Centralized management for the new firewalls is [not required].

Firewall Configuration and Migration

5. Like-for-like or redesign
Response: Primarily a like-for-like migration of existing policies, objects, NAT, routing, and VPN configuration, translated from FortiOS to PAN-OS, preferred. MISD expects cleanup of unused and shadowed rules during migration, and implementation of the security subscriptions included in the bid (see items 9 through 16). No full policy redesign is required.

6. Rule, object, and interface counts
Response: Current counts (DC / DR). Central NAT is enabled on both, and VDOMs are not in use.
• Firewall policies: 117 / 91
• Central SNAT rules: 48 / 24

• Central SNAT rules: 43 / 24
• Virtual IPs (destination NAT): 68 / 6
• IP pools: 60 / 16
• IPv4 address objects: 5,827 / 5,559, including 1,865 / 1,793 FQDN objects. These include the Texas-mandated prohibited technology blocklist (FQDN and ASN-based CIDR objects), built as address objects, not external feeds.
• IPv6 address objects: 3 / 3
• Address groups: 115 / 91
• Custom services: 366 / 325
• Service groups: 65 / 64
• Static routes: 23 / 12
• Policy routes: 0 / 0
• Local-in policies: 1 / 0
• Zones: 0 / 0. Policies reference interfaces directly, so security zones will need to be designed and built during migration.
• Interfaces (physical, aggregate, tunnel, and other logical interfaces): 48 / 46. No VLAN subinterfaces are configured on the firewalls.
• VDOMs: not enabled (single root VDOM on each)
7. BGP peers, site-to-site tunnels, and remote access users
Response:
• BGP peers: [2] at each site
• Site-to-site IPsec tunnels: [4], including a vendor tunnel to PowerSchool for database connectivity
• Remote access VPN: approximately [25] concurrent users at peak, [25] during emergency or closure scenarios
No changes to routing or VPN architecture are expected, other than moving remote access to GlobalProtect.

8. Additional capabilities in use
Response: Currently deployed and requiring migration:
• Remote access IPsec VPN (FortiClient) with Google Workspace SAML authentication at both sites
• Texas-mandated prohibited technology blocking using FQDN objects, ASN-based address lists, and Texas-ISAO threat feeds
• Web filtering: [yes]
• SSL/TLS inspection: [certificate inspection / deep inspection on specific segments]
• User identity integration: [LDAP]

Security Feature Implementation
9. Scope for security subscriptions
Response: License activation, migration of equivalent existing features, and baseline configuration aligned with best practices for each subscription. Items 10 through 16 describe the expectations for each feature.

10. Advanced Threat Prevention
Response: Vendor will migrate existing IPS profiles and any documented exceptions, then apply best-practice threat profiles. Existing customization is [minimal].

11. Advanced URL Filtering
Response: [Existing web filtering on the FortiGate will be migrated, and URL Filtering on the firewall will be configured as a secondary layer.] The prohibited technology blocklist must be maintained as custom categories or external dynamic lists and must remain updatable via the Texas-ISAO feeds.

12. Advanced DNS Security
Response: Baseline configuration with best-practice profiles. No third-party DNS integrations must be maintained beyond [internal DNS / any DNS filtering service].

13. Advanced SD-WAN
Response: SD-WAN is [not currently deployed]. MISD requires [subscription activation only / implementation across X circuits at the DC and DR sites].

14. Device Security
Response: Licensing, onboarding, and baseline device discovery and classification. Device-based policy enforcement is not required at deployment. Approximately [X] devices across [X] segments.

15. SSL/TLS Decryption
Response: [New implementation/migration of existing policy]. Vendor will configure decryption policy, certificates, and exceptions for [scope, e.g., staff and student internet traffic], with standard exclusions for financial, health, and certificate-pinned applications. MISD will provide the internal CA and handle certificate deployment to managed devices.

16. GlobalProtect / User-ID
Response: New implementation of GlobalProtect to replace the current FortiClient IPsec remote access, with SAML authentication through Google Workspace at both sites. Clients: Windows and macOS required. HIP checks are [not required]. User-ID integration with [Active Directory / Google] is [required].

17. Logging and monitoring integrations

17. Logging and monitoring integrations
Response: The new firewalls must support logging to [syslog local to the device] and API integration with NetBrain for monitoring. SNMP monitoring is required. Centralized logging through [Panorama / Strata Logging Service] is [not required].

Implementation and Cutover

18. Rack, power, cabling, and transceivers
Response: MISD will provide rack space and power. Vendor will include on-site rack mounting, cabling, transceivers listed in the bid, and physical connectivity.

19. Remote or onsite
Response: Configuration conversion and pre-staging can be performed remotely. Onsite engineering is required for installation and for each cutover.

20. Cutover windows
Response: All cutovers must occur after hours or on weekends during MISD-approved windows. MISD expects a phased migration: DR site first, then the primary data center after DR is validated.

21. Acceptance criteria and critical applications
Response: Beyond standard migration and failover testing, validation must include:
• Internet access for staff and student networks
• Remote access VPN login with SAML at both sites
• Site-to-site tunnels, including PowerSchool database connectivity
• State-mandated testing platforms (e.g., i-Ready) and other allowlisted applications
• Voice traffic for Webex Calling
• Prohibited technology blocking verified as enforced
• Failover from DC to DR for internet and remote access not in HA mode

22. Throughput, VPN, and decryption requirements
Response: Expected peak throughput is approximately [10] Gbps, with [20] Gbps of internet capacity at each site. Concurrent remote access VPN users are approximately [25] at peak. SSL/TLS decryption is expected on [50%] of traffic. The 25 Gbps minimum allows growth over the 5-year term with all subscriptions enabled.

Project Delivery and Knowledge Transfer
23. District IT availability
Response: Yes. MISD network staff will provide configuration access, coordinate network changes, process change management, and assist with application testing during cutover windows.

24. Completion date or schedule
Response: Work may begin after E-Rate funding commitment and MISD notice to proceed, no earlier than July 1, [2027]. Target completion is [to be determined after the bid is complete].

25. Training and knowledge transfer
Response: Vendor will provide as-built documentation, final configurations, and an operational handoff. MISD also requires [5 hours] of administrator knowledge transfer covering PAN-OS policy management, GlobalProtect, subscription management, and troubleshooting. Formal certification training is not required.

E-Rate: advanced subscriptions, GlobalProtect, Device Security, and centralized management are generally not eligible under Category 2. Vendors to break those out as separate line items for cost allocation.