



OFFICE OF PURCHASING AND DISTRIBUTION

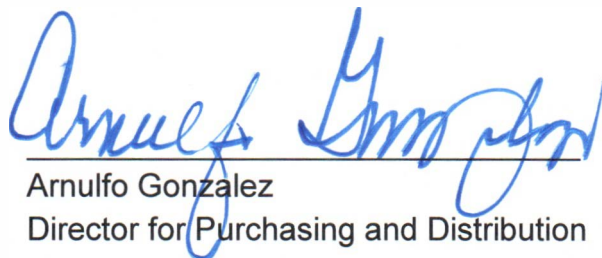
P.O. Box 110 • 801 Leopard Street
Corpus Christi, Texas 78403-0110
Office: 361-695-7350 Fax: 361-886-9192
www.ccisd.us

ADDENDUM #1 TO
FIREWALL REFRESH
DISTRICTWIDE (E-RATE YEAR 2027)
REQUEST FOR PROPOSAL (RFP#) FY27-P-0007

Date: October 12, 2026

The following items are hereby amended in RFP# FY27-P-0007:

- General Clarifications
- Questions and Answers


Arnulfo Gonzalez
Director for Purchasing and Distribution

All other terms and conditions remain unchanged.

If you should have any questions please contact Krystal.Garcia@ccisd.us

A COPY OF THIS ADDENDUM MUST BE SIGNED AND RETURNED WITH YOUR PROPOSAL:

NAME OF VENDOR ADDRESS/ZIP DATE

PRINT NAME/SIGNATURE OF REPRESENTATIVE TITLE

TELEPHONE NUMBER E-MAIL ADDRESS

**FIREWALL REFRESH
DISTRICTWIDE (E-RATE YEAR 2027)
REQUEST FOR PROPOSAL (RFP#) FY27-P-0007**

General Clarifications

Clarification 1 – SSL/TLS decryption throughput

Applies to: Cover page statement is unchanged; Section 7 (7.1.2.24 and the first two Scope of Work bullets); Worksheet 03 items 6.Y and 14

Amended language:

Section 7.1.2.24: “Minimum of 100 Gbps firewall throughput and a minimum of 90 Gbps SSL/TLS decryption throughput, each appliance of the HA pair must independently meet these minimums, with application control, intrusion prevention and anti-malware enabled simultaneously. Figures must come from the manufacturer’s published datasheet or test report, and the Offeror must state the metric name, test conditions and document/page cited.”

Scope of Work bullets: replace “and SSL/TLS decryption” with “and a minimum SSL/TLS decryption throughput of 40 Gbps.”

Worksheet 03 item 6.Y: replace “must sustain SSL/TLS with these features active” with “must sustain a minimum of 40 Gbps of SSL/TLS decryption throughput with these features active.”

Worksheet 03 item 14: replace “including SSL/TLS decryption” with “including a minimum of 40 Gbps SSL/TLS decryption throughput, with application control, intrusion prevention and anti-malware enabled simultaneously.”

Clarification 2 – Pricing period and Year 6 cost

Applies to: Worksheet 08 (Years 1–10); Worksheet 01 “On-going cost after Fifth year”

Amended language:

10 is retained as an evaluation-only year that does not extend the contract term. Five years of OEM support are required (Sections 7.1.2.2 and 11.3); later years are priced as support renewals.

The “On-going cost after fifth year for one additional year” in Worksheet 01 must equal the Year 6 cost in Worksheet 08 and must include all hardware support, security subscriptions, management, logging and software licenses needed to continue the solution at the same service level.

Clarification 3 – Remote-access VPN client

Applies to: Worksheet 03 item 8.G

Amended language:

“Solution must provide secure remote access for iPhone/iOS and Android devices. A manufacturer VPN application or the device’s built-in IKEv2 client is acceptable if it meets items 8.A–8.F. Offerors that do not support L2TP must so state, and describe how this requirement is met.”

Clarification 4 – Current firewall model

Applies to: Section 9.1; current network diagram

Amended language:

Section 9.1 and the diagram are corrected to read: “Firewall –FortiGate *3401E* in active and passive mode.”

Clarification 5 – Delivery date

Applies to: Worksheet 04 (Table: “What is your plan to deliver all services and equipment for the district by June 1, 2027”)

Amended language:

“What is your plan to deliver and install all services and equipment for the district by date – CCISD to set; must follow the Funding Commitment Decision Letter and the July 1, 2027 funding-year start, after confirming with the District’s E-Rate consultant. Offerors must not deliver or install before receiving written notice to proceed from the District.

Questions and Answers

Question 1: Sec. 11.2 “on-site support within 24 hours of request”: does this require the Offeror’s own engineer physically on site for any issue, or is OEM premium 24x7 support with advance hardware replacement delivered on site within 24 hours, plus 24x7 remote engineering, acceptable? Does the obligation run the full five years or only the installation and warranty period?

Answer:

Section 11.2 requires qualified technical support personnel on site within 24 hours of the District’s request when an issue cannot be resolved remotely. The District accepts OEM premium 24x7 support (Section 7.1.2) with advance parts replacement delivered and installed on site within 24 hours, together with 24x7 remote engineering from the Offeror or the OEM. The Offeror remains responsible for the response commitment, including when the OEM performs the work.

The obligation runs for the full five-year support and maintenance term (Sections 7.1.2.2 and 11.3), not only the installation or warranty period.

Question 2: Sec. 7.1.2.24, 7.1.2.4 and Worksheet 03 items 14 and 37: are the 100 Gbps firewall and 90 Gbps SSL/TLS decryption minimums per appliance or aggregate across the HA pair? Which published datasheet metric will the district use to verify them (for example SSL inspection throughput, threat protection throughput, or firewall throughput at a stated packet size), and must 90 Gbps decryption be sustained with IPS, antivirus and application control active simultaneously?

Answer:

The minimums apply per appliance. Each firewall in the HA pair must independently meet them, so that performance is not reduced after a failover. Throughput is not added across the two appliances.

The District will verify the figures against the OEM’s published datasheet or test report (RFP Section 7.1.2: required performance specifications must come from published public sources from production environments with all required features active). The 100 Gbps figure is the published throughput with application control, intrusion prevention and anti-malware enabled, and the 90 Gbps figure is the published SSL/TLS inspection throughput with those same services enabled. Offerors must identify the metric name, the test conditions (packet or transaction size, enabled services) and the document and page cited. See also Questions 28 and 29.

Question 3: Worksheet 04 asks for delivery by June 1, 2027, while the contract and funding year start July 1, 2027. Does the district expect equipment delivered and installed before the Form 471 funding decision? Will the district issue a purchase order before the

Funding Commitment Decision Letter, and will it pay the invoice in full if funding is delayed, reduced or denied?

Answer:

Worksheet 4 contains a clerical error in the date listed under "Timeliness to provide service." The correct date is **July 1, 2027**, in alignment with the funding year start date. *Subject to receipt of the Funding Commitment Decision Letter, the district may exercise the option to start Category 2 contracts as early as April 1*

Question 4: Sec. 7.1.2.2, 7.1.2.6, Worksheet 01 line 11 and Worksheet 08: should five years of OEM support and security subscriptions be priced as a single upfront five-year term (non-recurring) or billed annually (recurring)? Which Worksheet 01 line carries subscriptions, 03 Firewall or 05 Management Software? The Form 470 lists Internal Connections, BMIC and MIBS line items; which does the district intend to use for support?

Answer:

Offerors should price five years of OEM support and security subscriptions as a single upfront five-year term, shown on the same line as the hardware or software to which they apply (Worksheet 01 line 03 for the firewall and its subscriptions; the management line for management software and its subscriptions), with the annual cost for each year shown in Worksheet 08. Offerors may also show annual billing as an alternate option, labeled per Section 7.1.1. The Form 470 line item the District intends to use for support is *Internal Connections*. See Question 6 for the Worksheet 01 line structure.

Question 5: Sec. 6.1, 6.2 and 10.1: will the district state which pricing lines it treats as E-Rate eligible, or does each Offeror make that determination? For bundled NGFW subscriptions that include ineligible components (IPS, antivirus, URL filtering, sandboxing), does the district want a cost allocation per USAC guidance or separately priced SKUs?

Answer:

Each Offeror must identify, in Worksheet 01, the portion of each line that it believes is eligible and the portion that is ineligible under the current Eligible Services List, and must show how it reached that split. Where a bundle contains both eligible and ineligible components, Offerors should price separate SKUs where the manufacturer allows it, and otherwise provide a cost allocation consistent with USAC guidance. The District makes the final eligibility determination, with its E-Rate consultant, and may request changes to the allocation.

Question 6: Section 6.2.2 lists "Additional Services" and "Training and Certification"; Worksheet 01 lists "Management Device", "Management Software" and "Training". Which governs? Please also post the Excel versions of Worksheets 01 and 08 required by Note

4.2, and the Asset Register and Asset Transfer spreadsheets referenced in the appendices, which are not included in the PDF.

Answer:

The “Example” in 6.2.2 is purely an example. Use worksheet 01 for pricing as stated in the RFP, Worksheet 08 is Total cost over the years of ownership.

The District will not post the Excel versions of Worksheets, The offeror is to use the RFP tables as guidelines for building and attaching their own worksheets. Asset register and Asset Transfer examples are in the appendix.

Question 7: Sec. 7.1.1 and 3.6.6: if an Offeror submits labeled options (for example a second manufacturer, or a virtual East/West firewall in addition to the physical pair), should each option have its own complete Worksheet 01 and 08? Which option’s price is used for the 18, 21 and 10 price points, and is the East/West virtual option counted in total proposal amount or treated as an add-on?

Answer:

Yes. Each option must be labeled and have its own complete Worksheet 01 and Worksheet 08. For scoring of the 18-, 21- and 10-point price criteria, the District will use the Offeror’s clearly identified primary proposal: the physical HA pair for North/South traffic plus the Offeror’s recommended East/West solution. Other options are priced separately as alternates and are evaluated only if the District elects to consider them under Section 3.6.6. The East/West virtual option is part of the total proposal amount if it is part of the primary proposal; otherwise it is an alternate.

Question 8: For the East/West virtual/SDN firewall option, please describe the data center: number of Hyper-V hosts and clusters, Hyper-V version, approximate VM count, number of server VLANs or segments, expected East/West throughput, and any Azure footprint (VNets, ExpressRoute or VPN) to be protected. Is VM-level micro-segmentation required, or is VLAN-level segmentation through the physical HA pair acceptable?

Answer:

vSphere shows 43 networks configured, although some do not pass through the firewall as they are air-gapped iSCSI networks or VMWare specific traffic. Realistically, I believe around 10 of these actually go through the firewall.

VM-level micro-segmentation is / is not required. Offerors must describe how their proposed solution (virtual firewall, VLAN-level segmentation through the physical pair, or both) meets the District’s East/West security requirements, so the options can be compared. See also Question 31.

Question 9: The current network diagram shows a Lightspeed content filter inline between the firewalls and the Nexus core. Will Lightspeed remain in the same inline

position, or does the district intend the new firewall's URL filtering (Sec. 7.1.2.18, Worksheet 03 item 7) to replace it for CIPA compliance and HR user reporting?

Answer:

The Lightspeed content filter will remain in its current inline position / will be removed / position to be determined during design. The firewall's URL filtering and user reporting (Worksheet 03 items 7 and 35) remain requirements of the proposed solution. The firewall's URL filtering is intended to work alongside Lightspeed / replace Lightspeed for CIPA compliance and HR reporting.

Priority 2 – Migration and Design

Question 10: Sec. 9.1 says FortiGate 3104E; the diagram shows FG-3400/3401E. Please confirm the model, FortiOS version, whether FortiManager and FortiAnalyzer are in use, and the expiration date of the current support contract.

Answer:

The current firewall model is *3104E*. FortiOS version: Latest/up-to-date. FortiManager in use: yes. FortiAnalyzer in use: yes. Current support contract expiration date: July 1, 2027.

Question 11: Sec. 7.1.3.2 approximate number of firewall policies, address and service objects, NAT rules, VDOMs, site-to-site IPsec tunnels and concurrent remote-access VPN users. Is SSL inspection enabled today? Will a sanitized configuration export be provided after award?

Answer:

Yes. Because Section 7.1.2 requires the awarded Offeror to transfer the existing firewall rules, the District will provide a configuration export, with sensitive values removed, to the awarded Offeror after award.

Question 12: Sec. 7.1.2.1 and Worksheet 03 item 31: what interface speeds connect the firewalls to the ASR1002-HX routers and Nexus 7706 core today, and does the district plan to upgrade those links to 40 or 100 Gbps? Beyond four 10G SFP+ and eight 1G copper ports, are 25, 40 or 100G interfaces required? Does the Offeror supply transceivers for the Cisco side as well as the firewall side?

Answer:

Current links from the firewalls to the ASR1002-HX routers: 25gig QSFP x2 . Links to the Nexus 7706 core: QSFP . Planned upgrade to 40 or 100 Gbps: yes . Required 25/40/100G interface count and transceiver and connector types: 8 100gig.

Worksheet 03 item 31 states a minimum of four 10 Gbps fiber (SFP/SFP+) interfaces and eight 1 Gbps copper interfaces plus the interfaces needed for the HA link. Offerors must size interfaces so the proposed firewall can deliver 100 Gbps and must state the

interface counts and types proposed in Worksheet 03 technical specifications. Under Section 7.1.2, the Offeror is responsible for identifying and providing the correct fiber optics, fiber and cable lengths.

Question 13: Sec. 7.1.2.32 are the firewalls in NAT/route mode with dynamic routing (BGP or OSPF) to the ASRs and core, or static? Any VDOMs or VRFs to preserve? Preference for active/passive or active/active?

Answer:

Mode: Static. Routing to the ASR routers and core (BGP/OSPF/static): Static. VDOMs/VRFs to preserve: One.

Either active/passive or active/active high availability is acceptable (Section 7.1.2.32 and Worksheet 03 item 27). The District currently runs active/passive (Section 9.1). Offerors must state which mode they propose and how failover is achieved.

Question 14: Worksheet 03 items 4, 5, 6E and 33: number of AD domains or forests; is Google Workspace user identification required; current MFA provider; wireless controller platform; NAC in use.

Answer:

Worksheet 03 item 4 requires integration with Active Directory (multiple independent AD/LDAP domains) and Google Admin Console for user and group identification. Active Directory domains/forests: This proprietary information will be provided upon award. Google Workspace user identification: required (Worksheet 03 item 4). MFA provider: New MFA required or we can use any of our current solutions, currently use fortitoken for VPN access. Wireless controller platform: Cisco WLC. NAC in use: ISE.

Question 15: Sec. 7.1.2.23 and Worksheet 03 items L and X: which SIEM or log-management platform, expected log volume, and for the 3-, 6- and 12-month retention targets is an on-premises log appliance required or is cloud-hosted logging acceptable? Is a virtual management/analytics appliance on district Hyper-V acceptable for Worksheet 01 line 04?

Answer:

SIEM/log-management platform: CrowdStrike. Expected log volume: TBD, logs on firewall to be retained 90 days

Cloud-hosted logging is acceptable if the Offeror identifies the hosting location and includes all subscription costs for the term. A virtual management or analytics appliance on the District's Hyper-V environment is acceptable if the Offeror states the required compute, memory and storage and includes the license in the pricing. The retention requirements in Worksheet 03 item 6.X apply: three months readily searchable in the GUI, and at least six months of searchable offloaded logs, with twelve months preferred.

Question 16: Worksheet 03 item 8: is L2TP client support (8G) a hard requirement, or is a current SSL/IPsec client acceptable? Which identity provider is used for two-factor authentication of non-district users (8B)?

Answer:

The intent of item 8.G is secure remote access from iOS and Android devices. A current SSL or IPsec (IKEv2) client is acceptable if it meets items 8.A–8.F and the Offeror states how the requirement is met. Offerors who do not support L2TP must say so in their response. The identity provider used for two-factor authentication of non-District users is Provided by the firewall manufacturer.

Question 17: Sec. 7.1.3.3 which certification level and delivery format (on-site instructor-led, virtual, self-paced) for the four employees? Are OEM training credits or exam vouchers acceptable as “learning credits”?

Answer:

Section 7.1.2 requires vendor-specific training and certification for up to four District employees, with learning credits included for accredited testing. Certification level: administrator/professional level for the proposed platform. Delivery format: self-paced acceptable. OEM training credits and exam vouchers are acceptable if they cover the training and the accredited exam for four employees, and the Offeror states what they cover.

Question 18: Sec. 7.1.5 and 7.1.6: is summer break 2027 the intended cutover window? Any blackout dates? Is a parallel-run or rollback period required, and will district staff be on site for off-hours cutover and acceptance testing?

Answer:

Section 7.1.6 requires installation off school hours with two weeks’ notice. The intended cutover window is June 15 - July 1 2027. Parallel-run/rollback period: July 1 – July 31 2027. District staff will be on site for off-hours cutover and acceptance testing: Yes.

Question 19: Confirm the HA pair is installed only at the Technology Services Center, 2525 Belton St., with no secondary or DR data center firewall in scope.

Answer:

The HA pair is installed at the Technology Services Center, 2525 Belton St. No secondary or disaster-recovery data center firewall is in scope.

Question 20: Sec. 7.1.11: FRN line numbers are not known until the funding decision. May electronic asset tags be applied or updated after the FCDL?

Answer:

Yes. Asset tags may be applied at installation and the FRN line number, funding year and school number updated in the asset register after the Funding Commitment

Decision Letter. The register must be complete before final acceptance and final invoicing.

Question 21: Scope bullet 5 and Sec. 6.2.2 line 04: does the district want optional complementary services priced (sandboxing, email security, zero-trust remote access, SD-WAN), and are they scored?

Answer:

Optional complementary services that improve the security of the proposed solution may be priced on the “Additional Services” line, labeled as options (Section 7.1.1) and kept separate from the required solution. They are not separately scored; they may be considered in the evaluation of the technical approach and specifications to the extent they meet the District’s stated needs. The District has no obligation to purchase them.

Question 22: Worksheet 03 scoring references the Gartner Magic Quadrant 2019. Will the district accept the most recent Gartner Magic Quadrant for Network Firewalls or other current analyst reports?

Answer:

Yes. The Worksheet 03 reference to the 2019 Gartner Magic Quadrant is amended to “the most recent Gartner Magic Quadrant for Network Firewalls.” Other current independent analyst or third-party test reports may be submitted as supporting documentation.

Question 23: Worksheet 02: please define “comparable organization”. Do higher-education, municipal or county, or private-sector 100 Gbps firewall deployments qualify? Will projects completed by a named subcontractor count?

Answer:

A comparable organization is a K-12 school district, higher-education institution of similar size and complexity. Deployments of a firewall of 100 Gb throughput or larger qualify if the project description demonstrates similar type, size and complexity (Section 6.3.1 and Worksheet 02). Projects completed by a named subcontractor count only if that subcontractor is identified in the proposal and will perform work on this project.

Question 24: Standard Terms 16 and the Sample Contract “Assignment” clause: must subcontractors be identified in the proposal, and does acceptance of a proposal naming them constitute the district’s written consent?

Answer:

No, the district does not require prenotification of who the subcontractors will be.

Question 25: Standard Terms 18 and Sec. 13.7 to 13.9: will the district define “Contract Time” and accept a cap on damages? Are the bid, payment and performance bonds and the \$5M umbrella required of the prime Offeror only?

Answer:

“Contract Time” is the period established for delivery, installation and acceptance in the Contract Documents and the project schedule agreed with the District. The Notes to All Offerors require that exceptions to stated terms be addressed in writing with the proposal; the District does not agree in advance to a cap on damages and may consider requested exceptions under Section 3.6.7.

The bonds and the umbrella liability coverage in Section 13 are required of the prime Offeror.

Question 26: Sec. 3.2, Worksheet 01 line 11 and Worksheet 08 years 6 to 10: for the two optional three-year renewals, should years 6 and later be firm prices or OEM list less a stated discount?

Answer:

Section 3.2 requires proposals to be firm through the term of the award. Prices for years 6 and later must be stated as firm amounts or a firm, stated method (a fixed percentage increase or a fixed discount from a stated OEM price list), and Offerors must explain any anticipated increases in Worksheet 08. Price changes require thirty (30) days’ written notice and the District’s approval before they take effect.

Question 27: When does the district anticipate Board of Trustees award, given the Form 470 allowable contract date of Oct 28, 2026 and the Form 471 filing window?

Answer:

The District anticipates presenting the recommendation to the Board of Trustees on December 14, 2026. Proposals are due November 10, 2026 at 2:00 p.m. Award is subject to Board approval and E-Rate funding (Section 5).

Additional Questions

Question 28: Please confirm the required SSL/TLS decryption throughput. The cover states a minimum of 90 Gbps, while Sections 7 and Worksheet 03 reference SSL/TLS

decryption without consistently stating 90 Gbps. Is 90 Gbps mandatory with all required next-generation security services enabled?

Answer:

No. The District understands that turning on advanced services drops throughput. Minimum required throughput on north south traffic is 40gb.

Question 29: Please define the traffic profile and test conditions CCISD will use to validate the 100 Gbps firewall throughput and SSL/TLS decryption requirement, including packet size, cipher suites, transaction mix, enabled services, and whether published third-party or OEM results are acceptable.

Answer:

Published OEM datasheets and test reports, and published third-party test results, are acceptable (Section 7.1.2). The enabled services are application control, intrusion prevention, anti-malware and SSL/TLS decryption, active simultaneously. The District has not prescribed a packet size, cipher suite or transaction mix. Offerors must state the conditions of the test behind each published figure (packet or transaction size, cipher suites, traffic mix, enabled services). The District may request a demonstration or validation under realistic traffic conditions.

Question 30: Must the physical HA pair itself handle both North/South and East/West traffic, or may the mandatory physical HA pair handle North/South while a separately licensed virtual/SDN firewall handles East/West traffic?

Answer:

The mandatory physical HA pair is required for North/South traffic. East/West traffic may be handled by the physical pair or by a separately licensed virtual/software-defined firewall, as the Offeror proposes (cover page and Section 7). The Offeror must state which approach it proposes and price it separately in Worksheet 01.

Question 31: Please provide the expected East/West traffic volume, number of protected data-center segments/hosts, hypervisor platform and version, Azure footprint, and required number of virtual firewall instances.

Answer:

See Question 8. Required number of virtual firewall instances: 0

Question 32: Please provide the current network diagram in a legible electronic format and identify current routing, VLANs, zones, HA links, upstream/downstream devices, and demarcation points.

Answer:

The District provided the current network diagram in the RFP

Question 33: Please provide current and projected peak Internet, East/West, VPN, concurrent-session, new-session-per-second, and SSL/TLS inspection utilization, plus expected growth over the five-year support period.

Answer:

The District's Internet connectivity is two 15 Gb providers (Section 9.2). Offerors must size the solution to deliver the stated minimums with all features enabled. Will be upgraded at same time to two 20 Gb providers.

Question 34: Worksheet 03 requires at least four 10 Gbps fiber interfaces and eight 1 Gbps copper interfaces, but the solution must sustain at least 100 Gbps. Please confirm required 40/100 Gbps interface counts, transceiver types, connector types, fiber type, and whether optics must be included.

Answer:

See Question 12. Optics for the interfaces proposed must be included in the price (Sections 7.1.2 and 8.2.1).

Question 35: Will CCISD provide data-center site access or a detailed rack/fiber survey before proposals are due so bidders can determine optic types, cable media, cable lengths, rack units, power feeds, and cable-management requirements? If not, what assumptions should bidders use?

Answer:

The District Will provide site access before the project kickoff at customers convenience. If not provided, Offerors must state the assumptions used for optics, cable media and lengths, rack units and power, and must identify any additional requirements in writing per Section 8.2.2 and Section 7.1.2.10 (installation requirements 90 days in advance).

Question 36: Please confirm whether log storage sufficient for three months of readily searchable data and six months of offloaded searchable data must be included in the base price, and provide the current or estimated daily log volume and preferred twelve-month retention requirement.

Answer:

Yes. Storage and licensing sufficient for three months of readily searchable data and six months of searchable offloaded data (Worksheet 03 item 6.X) must be included in the base price. Twelve-month retention is preferred and may be priced as an option.

Question 37: Please identify the District's current SIEM/log-management and third-party security policy/change-management platforms, including supported integration methods and required use cases.

Answer:

SIEM/log-management platform: CrowdStrike. Security policy/change-management platform: self hosted by the district. Worksheet 03 item 23 requires support for third-party platforms through standard methods (API, syslog or configuration export); the District does not require a specific platform. Required use cases: log forwarding to the SIEM (Section 7.1.2.23 and Worksheet 03 item 6.L), alerting, and audit reporting.

Question 38: Please identify the versions/tenants of Active Directory, Google Admin Console, Microsoft 365 SMTP, wireless controllers, NAC, proxies, and other identity sources that must be integrated.

Answer:

Proprietary information will be provided upon award of contract. These should all be treated as such and considered to be on the latest versions of software. Specifics will not be provided on a public forum in accordance with our Security Standards.

Question 39: Please provide the required maximum numbers of site-to-site and remote-access VPN users/sessions, current VPN technologies, identity provider, MFA platform, certificate authorities, and any non-district-user access requirements.

Answer:

Proprietary information will be provided upon award of contract. These should all be treated as such and considered to be on the latest versions of software. Specifics will not be provided on a public forum in accordance with our Security Standards.

Question 40: Please provide the approximate number of existing firewall rules, objects, NAT policies, VPNs, virtual domains/contexts, and years of configuration/log data that must be migrated from the Fortigate 3104E environment.

Answer:

See Question 11. Years of configuration/log data to be migrated: current configuration only.

Question 41: Worksheet 04 requests delivery of all equipment and services by June 1, 2027, while the initial contract term begins July 1, 2027. Please confirm the intended

contract award, shipment, installation, cutover, acceptance, invoicing, and service-start dates.

Answer:

See Question 3. The District will confirm the contract award, shipment, installation, cutover, acceptance, invoicing and service-start dates by addendum.

Question 42: Please provide the expiration date and support/licensing end date of the existing firewall contract referenced in the required transition plan, including any blackout periods or mandatory cutover windows.

Answer:

See Questions 10 and 18. Existing firewall support and licensing end date: July 1 2027

Question 43: Please provide the mandatory acceptance-test criteria, duration, traffic-generation method, success thresholds, failover tests, security-service tests, and required documentation.

Answer:

Section 7.1.5 requires a mandatory performance evaluation by the Offeror in the presence of the District's authorized representative, proving full activation of the installed devices.

Question 44: The pricing categories in Section 6.2.2 differ from Worksheet 01—for example, Additional Services and Training and Certification versus Management Device, Management Software, and Training. Which pricing form and line-item structure governs the submitted Excel pricing proposal?

Answer:

See Question 6. The corrected pricing form issued by addendum governs.

Question 45: Please confirm which products and services CCISD expects bidders to classify as E-Rate eligible versus ineligible, and whether bidders should provide SKU-level quantities, unit prices, term lengths, discounts, taxes, shipping, and installation allocations in addition to the summary lines.

Answer:

See Question 5. In addition to the summary lines, Offerors must provide a SKU-level price list in the Excel pricing proposal showing quantities, unit prices, support/subscription term lengths, discounts, shipping and installation allocations. The District is tax exempt (Section 3.3) and taxes should not be included.

Question 46: The stated award structure is an initial three-year term plus two three-year renewal options, totaling nine years, while Worksheet 08 requests costs through Year 10.

Please confirm the intended pricing and licensing period for the ten-year TCO and whether Year 10 is an evaluation-only extension.

Answer:

The total of the initial term and both renewal options is nine years. The Worksheet 08 form will be corrected by addendum to. Five years of OEM support are required (Sections 7.1.2.2 and 11.3); later years are priced as support renewals.

Question 47: Please clarify whether the “ongoing cost after fifth year for one additional year” in Worksheet 01 should equal Worksheet 08 Year 6 cost and whether it must include all hardware support, subscriptions, management, logging, and software licenses.

Answer:

Yes. The “on-going cost after fifth year for one additional year” in Worksheet 01 must equal the Year 6 cost in Worksheet 08, and must include all hardware support, security subscriptions, management, logging and software licenses needed to continue the solution at the same service level.

Question 48: Several scoring references conflict: experience is shown as 8 or 10 points, and technical approach references 14 or 16 points. Please confirm the controlling evaluation weights and the exact maximum points for every criterion.

Answer:

Section 4.1 controls: total proposal amount 18; amount for eligible services 21; experience with similar projects 8; equipment specifications and technical documents 10; management plan 8; technical approach 14; HUB 3; previous experience with the District 8; total long-term cost 10 (100 points total). Section 6.3.1, the heading and text of Section 6.7, and the Worksheet 08 scoring language will be corrected by addendum to match.

Question 49: Section 6.3 says up to five projects, while scoring appears capped at four projects/eight points. Should bidders submit four or five comparable projects, and must each have been completed within five years of the proposal due date?

Answer:

Offerors should submit four comparable projects; two points are awarded for each, for a maximum of 8 points (Section 4.1). The reference to “up to five projects” in Section 6.3.1.1 will be corrected by addendum. Each project must have been completed within five years of the proposal due date of November 10, 2026.

Question 50: For each Worksheet 03 requirement, may bidders cite an attached datasheet/white paper by document name and page number rather than repeating the full

technical explanation? Please also confirm whether electronic worksheet responses may expand beyond the provided page layout.

Answer:

Yes. Offerors may cite an attached datasheet or white paper by document name and page number if the cited page directly answers the requirement. A brief statement of compliance and any caveats must still be entered in the response block (Section 6.7.2). Electronic worksheet responses may expand beyond the page layout; the worksheet's numbering and order must be preserved.

Question 51: Please confirm when the 90-day power/space notice is measured from and provide the required asset-tag format, E-Rate FRN line number, school number, room naming convention, and electronic asset-register template.

Answer:

Section 7.1.2.10 requires installation requirements (electrical and space) to be provided 90 days before installation, measured from the District-approved installation date. The District will provide the asset-tag format, FRN, school number and room naming convention to the awarded Offeror, and the electronic Asset Register template with the addendum.

Question 52: Please confirm the acceptable bid-bond form and surety requirements, and whether the 5% bid bond threshold is based on total proposal value, eligible value, initial term value, or ten-year TCO.

Answer:

This is the total eligible value for the project.

Question 53: Will CCISD accept carrier/courier delivery before the due date, and what recipient, office hours, labeling, and proof-of-receipt instructions should be used for delivery to the basement Purchasing office?

Answer:

Yes. Proposals may be mailed or hand delivered (Section 2.1) by courier before the due date. Deliver to the Corpus Christi Independent School District, Office of Purchasing and Distribution, basement, 801 Leopard Street, Corpus Christi, Texas 78401. Attention: Arnulfo Gonzalez. Proposals are time stamped on receipt and late proposals are returned (Section 2.2). Proof of receipt: The envelope must show the vendor's name, address, proposal title and proposal number (Section 2.1).

Question 54: Please provide an example of the exact required PDF, Excel, USB, outer-envelope, and separate-pricing-envelope file/label names, including punctuation and placement of the vendor SPIN and vendor name.

Answer:

The names are set in Notes 4.1 and 4.2: PDF file: "Firewall Upgrades Districtwide (E-Rate Year 2027) #FY27-P-0007 Your SPIN #123456789." Excel pricing file: "Firewall Upgrades Districtwide (E-Rate Year 2027) #FY27-P-0007 Your SPIN #123456789 and Offeror Name – Pricing Proposal." The separate pricing envelope uses the same text as the Excel file name. Replace the SPIN example with your own SPIN and "Offeror Name" with your company name. The USB drive and outer envelope use the PDF name, with the vendor's name and address and the proposal number on the outer envelope (Section 2.1).

Question 55: Please confirm where addenda will be posted, whether vendors must acknowledge every addendum within the proposal, and whether updated worksheets issued by addendum supersede the current forms.

Answer:

Addenda will be posted on the District's website under "Purchasing – Bidding Opportunities," and Offerors are responsible for obtaining them (Section 3.6.4). Offerors must submit all signed addendum pages with the proposal (cover page). Worksheets and forms issued by addendum supersede the corresponding forms in the original RFP.

Question 56: Will CCISD give evaluation consideration under Equipment Specifications and Technical Documents or Technical Approach for AI/ML-powered firewall capabilities—such as behavioral analytics, anomaly detection, automated threat correlation, policy recommendations, and autonomous response—when supported by measurable performance evidence? If so, please identify the capabilities, use cases, and evidence that evaluators will prioritize.

Answer:

The RFP already requires behavioral and anomaly-based analysis and advanced monitoring (Section 7.1.2.23 and Worksheet 03 item 6.M). Offerors may describe additional capabilities under Equipment Specifications and Technical Documents (Section 6.5) and Technical Approach (Section 6.7), and the District evaluates them to the extent they meet the District's stated needs. No separate scoring category or additional points are created for any particular technology. Evidence should be measurable and independent where possible, such as published test results, datasheets and documented use cases.

Question 57: Throughput (Section 7.1.2.24 and Worksheet 03 item 14). The RFP requires “a minimum of 100 Gbps firewall throughput, with SSL/TLS decryption,” and Worksheet 03 lists 90 Gbps of SSL/TLS decryption. Please confirm how performance figures will be evaluated: (a) must 100 Gbps be achieved with all security features (application control, intrusion prevention, anti-malware and decryption) enabled at the same time, or is 100 Gbps a firewall throughput figure with decryption evaluated separately; and (b) what SSL/TLS decryption throughput is required, and will the manufacturer’s published figures and test conditions be accepted as the basis?

Answer:

(a) The 100 Gbps minimum applies with the next-generation features required by the RFP enabled simultaneously: application control, intrusion prevention, anti-malware and SSL/TLS decryption (Section 7.1.2: “All required performance specifications shall be from published public sources from production environments with all required features and applications simultaneously active,” and Worksheet 03 item 14). It is not a firewall-only figure with decryption evaluated separately.

(b) The RFP cover page states a minimum SSL/TLS decryption throughput of 90 Gbps. Section 7.1.2.24 and Worksheet 03 item 14 say only “with SSL/TLS decryption,” and Worksheet 03 does not list 40 Gbps; it asks offerors to report their own figure in technical specification line J. Amendment: Section 7.1.2.24 and Worksheet 03 item 14 are amended to conform to the cover page and require a minimum of 40 Gbps SSL/TLS decryption throughput, with application control, intrusion prevention and anti-malware enabled simultaneously. Offerors must report their figures in Worksheet 03, technical specification lines H, I and J.

Manufacturer-published datasheets and test reports are accepted as the basis, provided they come from published public sources, identify the metric name and test conditions (features enabled, traffic mix, packet or transaction size), and match the proposed model. Offerors must cite the document and page. The District may request the test methodology and may request a demonstration.

Question 58: Traffic mix. Of the 100 Gbps requirement, roughly how much is expected to be Internet traffic versus server-to-server (east/west) traffic, and is 100 Gbps a firm minimum for the physical pair or a target for the combined physical and virtual solution?

Answer:

100 Gbps is a firm minimum for the physical high-availability pair that handles North/South (Internet) traffic. It is not a combined target with the virtual solution. The virtual/software-defined option for East/West traffic is proposed separately, sized by the offeror to the environment described in the response to Question 5, and does not count toward the 100 Gbps minimum. The Section 7 Scope of Work language that describes a single platform for both traffic types will be conformed to the cover page by addendum.

Proprietary information will be provided upon award of contract. These should all be treated as such and considered to be on the latest versions of software. Specifics will not be provided on a public forum in accordance with our Security Standards.

Question 59: Session capacity. Does the district have minimum requirements for concurrent sessions, new connections per second, or VPN throughput, and is there a required number of remote-access VPN users? None are stated in Worksheet 03.

Answer:

The RFP does not set minimum values for these. Offerors must report their proposed model's values in the Worksheet 03 technical specifications (including maximum sessions, new sessions per second, concurrent TCP sessions and IPsec VPN peers) and must size the solution to deliver the stated minimums with all features enabled. Remote-access VPN user counts are provided in the response to Question 10.

Question 60: East/west security requirements (Section 7). Are specific security features required for north/south (Internet) traffic versus east/west (server-to-server) traffic? For example, must intrusion prevention, anti-malware inspection and SSL/TLS decryption apply to east/west traffic, or is access control between server networks sufficient? Should the proposed firewalls handle east/west traffic in transparent (Layer 2) or routed (Layer 3) mode?

Answer:

The RFP does not distinguish features by traffic direction. The requirements in Section 7.1 and Worksheet 03 apply to the proposed solution as a whole. Offerors must state clearly which features are included for East/West traffic and which are separately licensed, so offers can be compared.

Offerors must state which deployment modes are supported for East/West traffic (transparent/Layer 2 and routed/Layer 3). CCISD has no preference.

Question 61: Virtual environments (Section 7). For the virtual/software-defined firewall option, please describe all virtual environments to be protected: which hypervisors are in use (for example VMware and Hyper-V), the number of hosts and approximate number of virtual machines in each, and the server networks to be segmented. What is hosted in Azure, how is it connected, and what type of integration with Azure is the district looking for (for example an Azure-hosted virtual firewall, or integration with Azure identity and networking only)?

Answer:

Worksheet 03 items 15 and 16 require the solution to be capable of implementation in multiple virtual and cloud environments, with Hyper-V integration and Azure preferred. The District's environment is:

Proprietary information will be provided upon award of contract. These should all be treated as such and considered to be on the latest versions of software. Specifics will not be provided on a public forum in accordance with our Security Standards.

Question 62: Management platform (Worksheet 03). May the central management and logging platforms be deployed as virtual machines (and on which hypervisor or cloud), or does the district require physical or cloud-hosted appliances?

Answer:

Yes. Central management and logging may be provided as virtual machines or as physical appliances. They may run on the District's VM ware, if the offeror states the required compute, memory and storage; a cloud-hosted management platform is also acceptable if the offeror identifies the hosting location and includes all licensing and subscription costs for the term. In all cases the platform must meet Worksheet 03 items 21 and 35 (single-pane management and centralized reporting) and the log retention in the response to Question 13.

Question 63: Decryption scope (Sections 7.1.2.9 and 7.1.2.13). Please describe the intended scope of SSL/TLS decryption: outbound user traffic, inbound traffic to district-hosted services, or both; whether the district operates its own certificate authority and already distributes certificates to managed Windows, Chromebook and iOS devices; how guest and personal devices should be handled; which categories (for example health and financial sites) must be exempt; and which collaboration or cloud applications must be scanned for malware and may be decrypted.

Answer:

Scope: the RFP requires decryption of both outbound and inbound SSL/TLS traffic (Section 7.1.2 and Worksheet 03 item 6.Y), applied by policy. The solution must also support the application-based rules and the malware scanning in allowed collaboration applications described in Section 7.1.2.

Question 64: Content filtering (Section 9; Worksheet 03). Will the Lightspeed content filter remain in place after the refresh? Is the firewall's URL filtering intended to replace Lightspeed as the district's CIPA filter, work alongside it, or cover only staff and server traffic? Do the per-user browsing history reports need to cover student devices, including off-campus use?

Answer:

The current network diagram shows the Lightspeed content filter inline between the firewalls and the core. After the refresh the content filter will remain in that position]. The firewall's URL filtering is intended to work alongside. Worksheet 03 item 7 (URL filtering and logging) remains a requirement of the proposed solution regardless. Per-user browsing history reports (Worksheet 03 items 7.B and 35) are required for users

the firewall can identify on the District network; off-campus student devices are not expected to be covered by the firewall.

Question 65: User identity. Which identity sources should the solution use for user-based policies and per-user reports (on-premises Active Directory, Microsoft Entra ID, Google Workspace for students)? Does the district have a network access control or wireless platform that can provide user-to-device mapping? Approximately how many students, staff and concurrent devices should be planned for?

Answer:

Worksheet 03 item 4 requires integration with Windows Active Directory (multiple independent AD/LDAP domains) and Google Admin Console for user and group information. Worksheet 03 item 33 requires offerors to list the wireless controllers supported for passing authentication information, and item 6.E requires integration with 802.1X, proxies and NAC.

Question 66: VPN (Section 7.1.2.19; Worksheet 03). (a) How many site-to-site tunnels and remote-access users (named and peak concurrent) should be planned for, and which multi-factor authentication platform does the district use today? (b) Worksheet 03 lists “L2TP for iPhone/Android”; would the manufacturer’s VPN app for iOS and Android, or the devices’ built-in IKEv2 client, satisfy this requirement? (c) Remote-access VPN clients are commonly licensed per user; how should offerors present that licensing given the per-appliance licensing requirement? (d) Is Suite-B encryption required for all tunnels, or only available on request?

Answer:

Proprietary information will be provided upon award of contract. These should all be treated as such and considered to be on the latest versions of software. Specifics will not be provided on a public forum in accordance with our Security Standards.

(b) Item 8.G is intended to ensure secure remote access from iOS and Android devices. A manufacturer VPN app or the built-in IKEv2 client is acceptable if it meets items 8.A–8.F and the offeror clearly states how the requirement is met. Offerors who do not support L2TP must say so in their response. This change is included in the addendum.

(c) Section 7.1.2 requires pricing based on appliance throughput and does not consider per-user or per-object licensing. If a remote-access VPN client requires per-user licensing, the offeror must size it to the user counts in (a), include it in the fixed price in Worksheet 01, and identify it in the “included in base price” column in Worksheet 03. The offeror may not charge additional per-user fees during the term.

(d) Worksheet 03 item 8.C requires the solution to support Suite-B GCM-128 and GCM-256. Support is required; use on all tunnels is not required.

Question 67: CASB integration. The RFP requires the “ability to integrate with a cloud access security broker (CASB) to provide data protection, regardless of location (on-premise, virtualized, private or public cloud such as Azure or AWS).” Is a CASB, or integration with one, a required part of this solution or a desired capability? Does the district have a CASB in use, or a preferred CASB, that the firewall must integrate with, and what form of integration is expected (for example log forwarding for cloud-app discovery or policy integration)?

Answer:

Worksheet 03 item 6.C is a capability requirement: the proposed solution must be able to integrate with a CASB. The District is not requiring offerors to supply a CASB, and no specific CASB is required. Offerors should describe the integration methods supported (for example log forwarding, API or policy integration) and identify any additional licensing cost.

Question 68: Policy management and audit platforms. The RFP says the solution “must support integration with third-party network security policy management / change-management and audit platforms, for continuous compliance and audit readiness.” Is this a requirement for the proposed solution or a desired capability? Does the district have, or require, a specific platform (for example Tufin, AlgoSec, FireMon or Skybox) that the firewall must integrate with or be supported by?

Answer:

Worksheet 03 item 23 is a requirement of the proposed solution: it must support integration with third-party policy management, change-management and audit platforms through standard methods (for example API, syslog or configuration export). The District does not require a specific platform, and the RFP does not name one. The District does not currently use such a platform. Offerors should list the platforms they support.

Question 69: Investigative reporting and log retention (Worksheet 03). The RFP requires the “ability to perform investigative reports for a minimum of three months of usage.” Must those three months of events be stored and searchable within the firewall management platform itself, or may a separate logging platform (the district’s SIEM or one included in the proposal) hold them with reports generated from there? Is retention beyond three months required, and do the per-user browsing history reports also need to cover the full three months?

Answer:

Worksheet 03 item 6.X requires the management interface (GUI) to maintain a minimum of three months of readily accessible, searchable logs, and a minimum of six months of searchable log data for logs that are offloaded or stored externally, with a preference for twelve months. Investigative reports (item 35.K) and per-user

browsing history reports (item 7.B) must cover at least three months and must be generated from data that is searchable in the platform supplied with the proposal. A separate logging/reporting platform included in the proposal may hold the data and generate the reports if it is priced in Worksheet 01 and meets items 21 and 35. Reports generated solely from the District's SIEM do not satisfy this requirement. Storage and licensing for the required retention must be included in the base price; twelve-month retention may be priced as an option.

End of Questions and Answers