

**FRIENDSHIP PUBLIC CHARTER SCHOOL
REQUEST FOR PROPOSALS FOR
FCC Cybersecurity Pilot Program – Eligible Products and/or Services
FCC Form 470# CBR420250081**

Friendship is soliciting proposals and qualification statements from parties having specific interests and qualifications in the areas identified in this solicitation. A selection committee will review and evaluate all qualification statements and proposals and may request that the bidders make oral presentations and/or provide additional information. The selection committee will rely on the qualification statements, proposals, additional information if provided and oral presentations if made, in the selection of finalists and, therefore, bidders should emphasize specific information considered pertinent to this solicitation and submit all information requested.

Interested parties must email the response to this RFP to: Ruby Sherman (ProcurementInquiry@friendshpschools.org) and E-Rate Central (Cybersecurity@e-ratecentral.com) no later than the date indicated below. The email subject line should clearly state "Form 470# BCR420250081 RFP Response".

Procurement Inquiry

Ruby Sherman
Friendship Public Charter School (FPCS)
1400 1st Street, NW Suite 300
Washington, DC., 20001

RFP Response due by 4pm EST, Tuesday, July 15, 2025. Late proposals will be disqualified.

You must sign below in INK; failure to sign WILL disqualify the proposal.

Company Name: _____

Company Address: _____

City, State, Zip Code: _____

Taxpayer Identification Number (T.I.N.): _____

Service Provider Identification Number (SPIN): _____

Telephone: _____ Fax: _____

Email: _____

Print Name: _____ Signature: _____

Your signature attests to your proposal to provide the goods and/or services in this proposal according to the published provisions of this Request for Proposal unless modifications or alterations are clearly noted in your proposal submission.

Friendship Public Charter School Inc. (“Friendship”) reserves the right to reject any and all qualification statements, to cancel this solicitation, and to waive any informalities or irregularities in procedure.

TABLE OF CONTENTS – REQUEST FOR PROPOSAL PACKAGE

The items below represent components, which comprise this Request for Proposal (RFP) package. Proposers are asked to review the package to be sure that all applicable parts are included. It is the Proposers responsibility to be thoroughly familiar with all Requirements and Specifications. Be sure you understand the following before you return your proposal packet.

1. **Cover Sheet:** Your company name, address, and your signature (**IN INK**) should appear on this page
2. **Table of Contents:** Identifies the order in which the information appears in the document.
3. **General Requirements:** You should be familiar with all of the General Requirements.
4. **Special Requirements/Instructions:** This section provides information you must know in order to make a complete and proper proposal.
5. **Specifications:** This section contains the detailed description of the products/services sought by Friendship Public Charter School.
6. **Attachments**
 - a. Proposal Requirement
 - b. Insurance Coverage Requirements
 - c. Financial Statements
 - d. Proposed Exceptions, Alterations, Additions, or Modifications to RFP (if any)

PROCUREMENT TIMELINE

Task	Due Date
Issue Date	Monday May 19, 2025
Deadline to Submit Non-Disclosure Agreement (NDA)	Friday May 30, 2025 at 4PM EST
Pre-Proposal Conference	Tuesday June 3, 2025
Deadline to Submit Questions	Friday June 6, 2025 at 4PM EST
Posting of Questions/Clarifications	Friday June 13, 2025
RFP Submission Deadline	Tuesday, July 15, 2025 at 4PM EST

GENERAL REQUIREMENTS

COMMUNICATIONS AND QUESTIONS

All communication with the FPCS regarding this RFP must be emailed and received by the "Deadline to Submit Questions" noted in the "Procurement Timeline." Questions should be directed to the RFP contacts identified on page one, with the Form 470 Number included in the subject line. Failure to include all contacts could result in questions going unanswered. Verbal inquiries are not allowed. Clarifications, when applicable, will be posted as an attachment/addendum to the RFP and Form 470. Each Offeror is responsible for downloading the current version of the Form 470 and attachments, including any addenda. Applicant reserves the right to ask vendors clarifying questions during the proposal review process.

Contact initiated by an Offeror concerning this solicitation with any other Applicant representative other than those listed as Form 470 contacts is prohibited. Unauthorized contact may result in the offeror's disqualification from this solicitation.

Product demonstration meetings will not be granted during the competitive bidding period – requests for such will be ignored.

ACCESS TO RECORDS

Proposer may be required to allow duly authorized representatives of FPCS access to contracts, books, documents, and records necessary to verify the nature, extent, and cost of services provided by the Proposer.

AWARD

FPCS reserves the right to reject any and all proposals and reserves the sole right at its discretion to accept any proposal(s) it considers most favorable to the interest of FPCS and waive any and all minor irregularities in any proposal(s). FPCS further reserves the right to reject any proposal(s) and seek new proposals through the issuance of a new or amended RFP if such action is deemed in the best interest of FPCS.

OFFER COMPLETION

Completed proposal(s) must be sent to ProcurementInquiry@friendshipschools.org and Cybersecurity@e-ratecentral.com. An authorized company representative should sign the Cover Sheet. Completion of these forms is intended to verify that the proposer has submitted the proposal, is familiar with its contents, and has submitted the material in accordance with all requirements.

The submission of a response shall be prima facie evidence that the Proposer has full knowledge of the scope, nature, quantity, and quality of work to be performed, the detailed requirements of the project, and the conditions under which the work is to be performed.

All terms, conditions, specifications, stipulations and supplier requirements stated in the RFP, any attached Appendices to the RFP, and any and all Addenda issued shall become part of the contract entered into between FPCS and the Proposer.

OFFER RETURNS

Proposers must return completed proposals by date stated above. Late proposals will not be accepted. It is the responsibility of the responding Proposer to assure that the response is received prior to the date/time indicated on the Cover Page of this package.

CONTRACT RENEWALS

Renewals may be made **ONLY** by written agreement between FPCS and the Proposer. Any price escalations are limited to those stated by the Proposer in the original proposal.

DISQUALIFICATION OF PROPOSER

Upon signing this offer document, a Proposer certifies that the proposal has not violated the antitrust laws of this state, Business & Commerce Code, or the federal antitrust laws, and has not communicated directly or indirectly the proposal made to any competitor or any other person engaged in such line of business. Any or all proposals may be rejected if FPCS believes that collusion exists among the proposers. Proposals in which the prices are obviously unbalanced may be rejected.

Proposals **must** be in response to the specific requirements of this solicitation. Offers including a generic listing of services beyond the scope of this solicitation and/or encyclopedic price lists will be disqualified. SPAM and/or robotic responses will not be considered valid responses and will be disqualified from consideration.

Offerors who propose and alternative solutions to what is requested in the Scope of Work section of this RFP and all associated RFP documents but fail to provide documentation which establishes the equipment is equivalent will be disqualified. The documentation must specifically demonstrate that a product offers similar functionality and performance to the equipment indicated in the RFP.

Offerors interested in responding to this RFP must submit their Non-Disclosure Agreement (NDA) but the date and time identified in the Procurement Timeline. Failure to submit an NDA will disqualify your proposal for further consideration.

EVALUATION

In evaluating the proposals submitted, FPCS will apply the “Best Value” process in selecting the Proposer to be awarded a contract for this project. **Purchase price is not the only criteria that will be used in the evaluation process; however, price will be primary as well as the factor carrying the highest weight.** The selection process will include, but not be limited to, the following considerations:

1. **Cost of eligible Cybersecurity equipment and services. 30 Points.**
 - a. Eligible Cost
2. **Total long-term cost to FPCS including ineligible costs. 5 Points.**
 - a. Ineligible cost

- b. Cost FPCS must incur to implement the solution not included in the proposal.
- 3. Technical Solution and Approach. 20 Points.**
 - a. Architecture: is the proposed technical architecture sound, scalable, and maintainable?
 - b. Methodology: Does the vendor outline a clear and well-defined implementation methodology?
 - c. Design Considerations: Are key design elements like security, data management, addressed adequately?
 - d. Risk Assessment and Mitigation: Does the vendor identify potential risks associated with the solution and outline clear mitigation strategies?
 - e. Contingency Planning: Are contingency plans for addressing unforeseen technical challenges included?
- 4. Meets/Understands Needs of RFP. 15 Points.**
 - a. Does the vendor incorporate all aspects of the desired Cybersecurity solution?
 - b. Scalability: Can the solution be scaled to accommodate future and changing business needs?
 - c. Data Protection: How does the solution protect sensitive data and comply with relevant data privacy regulations, and what security protocols and features are implemented in the solution?
- 5. Vendor Experience and References. 15 Points.**
 - a. Provided preferably five (5) references with K-12 Public School districts and large government organizations.
 - b. Technical Team: Does the vendor have a qualified technical team with relevant experience in the proposed solution?
 - c. Track Record: Provide examples of successful similar projects implemented by the vendor, showcasing their technical capabilities.
- 6. Compatibility with Existing Cybersecurity Infrastructure. 15 Points.**
 - a. The solution is compatible with current cybersecurity infrastructure and mechanisms in place.

The vendor selected will be determined as the offeror who scores the highest number of points based upon the criteria identified above.

All proposals must be valid for a minimum period of one hundred-eighty (180) days to up to one year from the due date of this RFP. Proposers shall furnish in a timely manner to FPCS such additional information as FPCS may reasonably require.

FPCS reserves the right to contact references from the Proposer's client list, or any other persons considered relevant by FPCS.

All costs associated with the project must be enumerated in the proposal. Any costs associated with the project not explicitly enumerated and discussed in the proposal will not be honored. Contract prices and terms are to remain firm through project completion. The Proposer shall provide information on their standard fee arrangement for any goods and/or services proposed, and any discounts offered.

DOCUMENT INTERPRETATION

In the event of any conflict of interpretation of any part of this overall document, the interpretation of FPCS shall govern consistent with the laws of the District of Columbia. Wherever the term “Proposer” is used throughout the RFP, it includes the Proposer’s agents, employees, directors and/or assigns even if not specifically delineated.

HOLD HARMLESS AGREEMENT

The successful Proposer(s), its agents, employees (paid or volunteer), directors and/or assigns shall indemnify, hold harmless, and defend FPCS, its directors, officers, and employees (paid or volunteer) from and against any and all claims, demands, causes of action of whatever kind or nature arising out of error, omission, misrepresentation, negligent act, conduct or misconduct of the Proposer and its agents, employees(paid or volunteer), directors and/or assigns in the provision of goods or the performance of services arising out of the preparation of this proposal and execution and performance of any contracts resulting there from. Such indemnification shall also include reasonable attorneys’ fees, court costs, and expenses.

INSPECTIONS

FPCS reserves the right to inspect any item(s) or service location for compliance with specifications, requirements, and the needs of FPCS. If a Proposer cannot furnish a sample of a proposed item, where applicable, for review, or fails to satisfactorily show an ability to perform, FPCS can reject the proposal as inadequate.

TESTING

FPCS reserves the right to test equipment, supplies, materials and goods proposed for quality, compliance with specifications and ability to meet the needs of FPCS. Demonstration units must be available for review. Should the goods or services fail to meet requirements and/or be unavailable for evaluation, the proposal is subject to rejection.

INVOICES AND PAYMENTS

The Proposer who is awarded the contract is required to send all invoices to FPCS’s reference point of contact and to **Accounts Payable 1400 1st Street NW Washington DC 20001**. Invoices shall be provided to FPCS in a timely manner. The Proposer who is awarded the contract is required to invoice FPCS within 30 days of providing goods and/or services to FPCS. FPCS prefers to use the SPI method of invoicing, so the proposer who is awarded the contract will be required to invoice USAC/FCC directly for the discounted portion. If SPI is used, FPCS will not be invoiced for the full amount of the products and/or services.

In the event FPCS is presented with invoices, statements, reports, etc. that are incomplete, or inaccurate, FPCS may be required to perform substantial research which could result in delay of payment. FPCS will not be responsible for any interest charges and/or late fees as a result of delayed payment due to time delays caused by inadequate, incomplete, or inaccurate information provided in invoices.

PRICING

Prices for all goods and/or services shall be negotiated to a firm amount for the duration of the contract or as agreed to in terms of time frame and/or method of determining price escalations, if any by Proposer. All prices and methods of determining prices must be written in ink or typewritten. Where unit pricing and extended pricing differ, unit pricing prevails.

SUPPLEMENTAL MATERIALS

Proposers are responsible for including all pertinent product data in the returned offer package. Literature, brochures, data sheets, specification information, completed forms requested as part of the offer package and any other facts which may affect the evaluation and subsequent contract award should be included. Materials such as legal documents and contractual agreements, which the Proposer wishes to include as a condition of the proposal, must also be in the returned proposal package. Failure to include all necessary and proper supplemental materials may be cause to reject the entire proposal.

TAXES

FPCS is exempt from federal, state and local taxes. In the event that taxes are imposed on the goods or services purchased, FPCS will not be responsible for payment of the taxes. The Proposer awarded the contract shall absorb the taxes entirely. Certificates of exemption will be furnished upon written request to FPCS.

CONTRACT TERM

Any contract which results from this RFP shall run for no more than a three-year period, which is the duration of the FCC's Cybersecurity Pilot Program. Any renewals after three years will not leverage any funding mechanism such as the FCC Cybersecurity Pilot Program. Accordingly, offerors are requested to provide pricing that does not exceed a three-year term; proposals which require a contractual term of more than three years will be disqualified.

The desired contract term resulting from this RFP is a total of three years with 1+1+1 being the preferred term.

The Cybersecurity Pilot Program has a budget for Friendship Public Charter Schools which is \$171,156.00. Any costs above this amount will not be funded as part of the Cybersecurity Pilot Program.

The successful Proposer, as determined by FPCS, shall be required to execute a contract to furnish all goods and/or services and other deliverables required for successful completion of the proposed project. No Proposer shall obtain any interest or right in any award until FPCS has executed a contract, and any such interest and rights shall be subject to the terms and conditions as contained in such contract.

The successful Proposer may not assign, sell, or otherwise transfer its interest in the contract award or any part thereof, without prior written consent from the FPCS.

QUANTITY

There is no guaranteed amount of business, expressed or implied, to be purchased or, contracted for by FPCS in the initial maximum 1 year contract term or in subsequent renewals which may or may not be negotiated and agreed to by FPCS with any proposer(s). However, the Proposer(s) awarded the contract shall furnish all required goods and/or services to FPCS at the stated price, when and if required.

CONTRACT TYPE

The preferred contract type to be awarded is a fixed fee contract. However, if a Proposer has reason to believe a better (more cost effective) method is practical, then the Proposer is encouraged to offer that better pricing option as an alternative in its submitted proposal. FPCS will consider that type of contract as it compares with other recommended contract options. The contract type providing the best value, over the longest period of time is what FPCS seeks. Proposers are required to provide FPCS with a menu of any optional services offered. Each service must be priced separately and independent of any other services offered or rendered.

TERMINATION

FPCS reserves the right to terminate the contract without cause with 60 days prior written notice for convenience and with 30 days prior written notice for cause, if Proposer breaches any of the terms therein, including warranties of proposer or if the proposer becomes insolvent or commits acts of bankruptcy. Such right of termination is in addition to and not in lieu of any other remedies which FPCS may have in law or equity. Cause may be construed as, but not limited to, failure to deliver the proper goods and/or services within the proper amount of time, and/or to properly perform any and all services required to FPCS's satisfaction and/or to meet all other obligations and requirements.

If the Proposer breaches any provision of the proposal stipulations, becomes insolvent, enters voluntary or involuntary bankruptcy, or receivership proceedings, or makes an assignment for the benefit of creditors, FPCS will have the right (without limiting any other rights or remedies that it may have in the contract or by law) to terminate any contract with 30 days prior written notice to the Proposer.

FPCS will then be relieved of all obligations, except to pay the reasonable value of the supplier's prior performance (at a cost not exceeding the contract rate). The Proposer will be liable to FPCS for all costs exceeding the contract price that FPCS incurs in completing or procuring the service as described in the proposal. FPCS's right to require strict performance of any obligation in this contract will not be affected by any previous waiver, forbearance, or course of dealing.

TRANSITION

Once an executed contract with the Proposer terminates for any reason, FPCS reserves the right to have a period of time to transition the contracted goods and/or services provided to FPCS by the Proposer to a new provider. During this transition period, FPCS will pay for these goods and/or services to the provider at the negotiated rate(s) in existence at that time. FPCS further reserves the right to establish the length of the transition period and communicate this transition time period to the provider; however, such transition period shall not exceed 180 days.

FUNDING OUT OPTION

Any contract resulting from this RFP is contingent upon the continued availability of budget appropriations and is subject to cancellation, without penalty to FPCS, either in whole or in part, if funds are not appropriated by the FPCS Board of Directors, or otherwise not made available to FPCS. All outstanding invoices will be paid upon cancellation.

WARRANTIES

Proposers shall furnish all data pertinent to warranties or guarantees which may apply to items in the proposal. Proposers may not limit or exclude any implied warranties.

ASSOCIATION

Proposers may not use the FPCS official logo(s), or any phrase associated with FPCS, without the written permission from FPCS.

EXCEPTIONS, ALTERATIONS, ADDITIONS AND MODIFICATIONS

If any exceptions, alterations, additions, or modifications are submitted by Proposer to any portion of this RFP, the Proposer must clearly indicate the exceptions, alterations, additions and modifications and include a full explanation as a separate attachment to the proposal. The failure to identify exceptions, alterations, or modifications will constitute acceptance by the proposer of the RFP as proposed by FPCS. FPCS reserves the right to reject a proposal containing exceptions, alterations, additions, or modifications.

PROPOSAL PREPARATION COSTS

All costs related to the preparation and submission of this proposal shall be paid by the Proposer. Issuance of this RFP does not commit FPCS, in any way, to pay any costs in the preparation and submission of the proposal, nor does the issuance of the RFP obligate FPCS to award a contract or purchase any goods and services stated in the RFP.

RETENTION OF PROPOSAL DOCUMENTATION

All proposal materials and supporting documentation that is submitted in response to this proposal becomes the permanent property of FPCS.

MODIFICATION/WITHDRAWAL OF PROPOSAL

Proposals may be modified in writing at any time prior to the due date. Proposals may be withdrawn in writing, by facsimile written transmission, or in person before the response date.

FCC CYBERSECURITY PILOT PROGRAM PROVISIONS

FCC rules require vendors to offer discounted SPI billing. The applicant requires SPI discount method for these services. Vendors that do not offer SPI billing will be disqualified.

By submitting a proposal on the requested services herein, the vendor certifies its proposed services and/or products comply with Part 47 Section 54.9 and 54.10 of the FCC rules which prohibits the sale, provision, maintenance, modification, or other support of equipment or services provided or manufactured by Huawei, ZTE, or any other covered company posing a national

security threat to the integrity of communications networks or the communications supply chain. See <https://www.usac.org/about/reports-orders/supply-chain/> for more details.

As required by Section 54.500(f) of Part 47 of the Code of Federal Regulation all bids in response to this RFP **must** offer the lowest corresponding price (LCP) which is defined as the lowest price that a service provider charges to nonresidential customers who are similarly situated to a particular E-Rate applicant (school, library, or consortium) for similar services. See <https://www.usac.org/E-Rate/service-providers/step-2-responding-to-bids/lowest-corresponding-price/> for more details.

The vendor submission is subject to open records requests and, as such, the records will be released in accordance with those policies. Vendors are encouraged to mark pages as “Proprietary” or “Confidential” as appropriate, but the entire submission may not be marked as such. Identifying information as “Proprietary” or “Confidential” does not guarantee that the information will not be released but will be considered in determining whether the information is required to be released in accordance with the open records policies. Generally, pricing is not exempt from being publicly released.

Offerors proposing equipment whose prices may increase depending upon new U.S. government tariffs imposed on imports are encouraged to (a) identify such products in their offers, and (b) propose an acceptable methodology for limiting price adjustments over the contract term.

SPECIAL REQUIREMENTS/INSTRUCTIONS

EVALUATION AND AWARD

This RFP in no manner obligates FPCS to the eventual rental, lease, and purchase, etc. of any equipment or service described, implied or which may be proposed, until confirmed by a written contract. Progress toward this end is solely at the discretion of FPCS and may be terminated at any time prior to the signing of the contract. FPCS may initiate discussions with supplier personnel authorized to contractually obligate the supplier. Discussions will develop into negotiating sessions with the successful Proposer(s).

If FPCS is unable to agree to contract terms, FPCS reserves the right to terminate contract negotiations with a Proposer and initiate negotiations with another Proposer. FPCS reserves the right to select services and products from any number of Proposers if in its sole discretion it is in the best interest of FPCS to do so. Evaluation will consider the proposal(s) best meeting the needs and requirements of FPCS and such evaluation and determination of best value shall be solely at the discretion of FPCS.

The Applicant reserves the right to request Best and Final Offers (BAFOs). BAFOs must be received by the date/time provided during discussions/negotiations, or the originally submitted proposal will be used for further evaluation and award recommendation. FPCS reserves the right to request a BAFO from up to and no more than five of the offerors who scored the highest number of points during the vendor selection process.

Purchase price is not the only criteria that will be used in the evaluation process; however, it will be the primary factor carrying the highest weight.

Submission of a proposal implies the Proposer's acceptance of the evaluation criteria and all other terms and conditions as set forth in this RFP as well as the Proposer's recognition that subjective judgments can and will be made by those individuals evaluating proposals.

FPCS RESERVES THE RIGHT TO AWARD THE CONTRACT TO ONE PROPOSER/CONTRACTOR, OR MORE THAN ONE PROPOSER/CONTRACTOR IN ITS SOLE DISCRETION.

NON-PERFORMANCE BY PROPOSER/CONTRACTOR

Performance, before and during the contract term, will be a major consideration of current contract award, renewals, and future award considerations. Failure to perform, in any sense relative to this contract, may result in the probation and/or termination of this agreement by FPCS on the basis of nonperformance. Nonperformance shall be determined as follows:

1. Failure to meet and maintain all qualifications required in this RFP;
2. Failure to meet required operating performance standards in the time period required and consistent with workmanlike manner. Workmanlike manner means work that is "completed in a skillful manner and is non-defective.";
3. Failure to keep and maintain all required insurance coverage;
4. Failure to cure deficiencies within a reasonable amount of time as stated herein.

INSURANCE

All proposers must provide evidence of insurance or insurability.

CONFLICT OF INTREST

The prospective proposer, its agents, employees, directors and/or assigns, shall disclose any financial, business or other relationship with FPCS that may have an impact upon the outcome of this contract or potential future of the FPCS projects resulting from this effort. The prospective proposer, its agents, employees, directors and/or assigns shall also list current clients who may have a financial interest in the outcome of this contract or FPCS projects that will follow. In particular, the prospective proposer its agents, employees, directors and/or assigns shall disclose any financial interest or relationship with any company that might submit a bid on the FPCS projects. **If applicable, please complete Attachment F.**

NON DISCRIMINATION

The selected proposer shall comply, and shall require its agents, employees, directors and/or assigns to comply, with all applicable federal, state, and local laws, ordinances, rules, and regulations in regard to nondiscrimination in employment because of race, creed, color, ancestry, national origin, religion, sex, marital status, age, medical condition, pregnancy, disability, or other prohibited basis.

NON-DISCLOSURE AGREEMENT

Parties interested in bidding on this RFP must provide a Non-Disclosure Agreement (NDA) to FPCS. This NDA must be submitted to Ruby Sherman (ProcurementInquiry@friendshipschools.org and E-Rate Central (Cybersecurity@e-ratecentral.com) by Friday May 30, 2025 at 4PM EST. FPCS intends to share certain confidential and proprietary information with offeror(s) for the purpose of evaluating and proposing cybersecurity equipment and related services to enhance FPCS' existing network infrastructure.

PRE-PROPOSAL MEETING

For this RFP, a pre-proposal meeting is: ☒ Required ☐ Optional ☐ Not Offered

A pre-proposal meeting will be held at 2:00 PM EST via Zoom video conference on Tuesday June 3, 2025. Offerors interested in attending should RSVP by June 2, 2025 to ProcurementInquiry@friendshipschools.org and Cybersecurity@e-ratecentral.com

Pre-Proposal Conference Information:

<https://friendshippcs.zoom.us/j/99634532233?pwd=79Xr99qvFXjiDHpjYWSkaQ0SDAbIxa.1>

Meeting ID: 996 3453 2233

Passcode: 835716

Offeror attendance is mandatory; failure to attend any required pre-proposal site visit will result in disqualification by the Applicant.

No additional information will be provided during the pre-proposal meeting. Questions must be submitted via email as instructed above and answers will be posted as an attachment/addendum to the Form 470.

[Remainder of this page intentionally left blank]

Summary & Synopsis – Current Environment

Friendship Public Charter School (FPCS) operates a hybrid IT environment supporting approximately 1,000 staff and 4,750 students across various physical locations, and a central head office.

All locations are currently connected via MPLS circuits, with a centralized primary data center located at one of the main campuses. As part of our upcoming network modernization, we plan to transition to an SD-WAN solution in Summer 2025 to enhance connectivity and performance.

In our current environment, staff devices primarily run Microsoft Windows and are managed under Active Directory. Students operate in a managed Google Workspace domain using Chromebooks, with certain grade levels using iPads managed through a Mobile Device Management (MDM) platform. We have one school site that utilizes Apple Mac devices for staff and classroom instruction. Staff email is hosted on Microsoft Office 365 Exchange Online.

The network infrastructure includes Cisco and Meraki switching and wireless equipment. A cloud-based firewall solution secures internet traffic, and content filtering is in place for all internet-bound traffic to ensure compliance with industry standards and internal policies. Student device traffic, both onsite and remote, is filtered through appropriate mechanisms.

FPCS uses Windows Servers as its primary server infrastructure, with some virtualization deployed across select sites. Security controls and administrative safeguards are in place to protect systems and data. Endpoint protection is provided via a cloud-based EDR solution, and email security is reinforced through a third-party cloud spam filtering service.

Onsite IT support is available across locations, supported by centralized infrastructure and cybersecurity leadership. Our security approach follows best practices, and through the FCC Cybersecurity Pilot Program, we aim to strategically enhance these capabilities.

[Remainder of this page intentionally left blank]

Friendship Public Charter School sites

Site Name	Address	City, State, Zip
Friendship Online*	1351 Nicholson Street NW	Washington, DC 20011
Friendship Armstrong Elementary & Middle**	111 O Street NW	Washington, DC 20001
Friendship Public Charter Schools Admin Building**	1400 1st Street NW	Washington, DC 20001
Chamberlain Elementary	1345 Potomac Avenue SE	Washington, DC 20003
Chamberlain Middle School	1345 Potomac Avenue SE	Washington, DC 20003
Tech Prep Academy	2705 Martin Luther King Jr. Avenue SE	Washington, DC 20032
Woodridge Elementary	2959 Carlton Avenue NE	Washington, DC 20018
Woodridge Middle School	2959 Carlton Avenue NE	Washington, DC 20018
Friendship Collegiate Academy	4095 Minnesota Avenue NE	Washington, DC 20019
Friendship Ideal Elementary	6130 N Capitol Street NW	Washington, DC 20011
Friendship Ideal Middle	6130 N Capitol Street NW	Washington, DC 20011
Friendship Southeast Elementary Academy	645 Milwaukee Place SE	Washington, DC 20032
Blow Pierce Elementary	725 19th Street NE	Washington, DC 20002
Blow Pierce Middle	725 19th Street NE	Washington, DC 20002
Ideal Northeast (aka Friendship Lamond Campus)	6200 Kansas Ave NE	Washington, DC 20011

*Denotes Network Operations Center

** Friendship Armstrong Elementary & Middle and Friendship Public Charter Schools Admin Building are one physical location and share one circuit.

[Remainder of this page intentionally left blank]

RFP SPECIFICATIONS – Services

Under the FCC’s Cybersecurity Pilot Program, Friendship Public Charter Schools has a three-year budget not to exceed \$171,156.00. Any costs above this amount will not be covered under the FCC Cybersecurity Pilot Program.

Friendship Public Charter Schools seeks qualified and experienced bidder(s) for Cybersecurity Equipment and Services limited to: 1) Endpoint Protection, 2) Identity Protection and Authentication, and 3) Monitoring, Detection, and Response.

Scope of required services to include but not limited to the following products and/or services.

Proposals will be accepted for the makes/models specified in this RFP and any associated RFP document. Offers that contain alternative makes/models are required to submit product specifications and documentation to establish that the equipment is equivalent to the requested solution. FPCS will be the arbiter of whether the proposed solution is functionally and technically equivalent to the requested solution. Offerors who propose an alternative solution but fail to provide documentation which establishes the equipment is equivalent will be disqualified. The documentation must specifically demonstrate that a product offers similar functionality and performance to the equipment indicated in the RFP.

Endpoint Protection				
Request #	Category	Product and Technical Specs Requested	Quantity Requested	Duration of Product/Service
EP1	Endpoint Detection and Response (EDR) Solution	Symantec (or equivalent) Endpoint Security Complete	1750 licenses	Annually - 3 Years Total
		Inclusive of product updates, upgrades, virus definition updates, and technical support.		
		Advanced threat protection for workstations and servers.		
		Zero-trust security model enforcement.		
		Centralized policy management and enforcement.		
		AI-powered malware, ransomware, and exploit prevention.		
		Behavioral analysis for anomaly detection.		
		Solution should include pre-attack surface reduction, attack prevention, and breach prevention.		
		Response and Remediation		

Identity Protection and Authentication				
Request #	Category	Product and Technical Specs Requested	Quantity Requested	Duration of Product/Service
IP&A 1	Email Security – Spam Guard & Phishing Protection	Barracuda (or equivalent) Email Gateway Defense with Cloud Archiving	1000 licenses	Annually - 3 Years Total
		AI-based filtering for spam, phishing, and malware.		
		Sandboxing for suspicious attachments and links.		
		DMARC, DKIM, and SPF enforcement for email authentication.		
		Real-time threat intelligence and adaptive filtering.		
IP&A 2	Active Directory, Email & File Server Auditing Solution	URL rewriting and malicious link detection.	1200 Licenses - File server License : 1 - Privileged Access Management License: 20	Annually - 3 Years Total
		Netwrix Auditor (or equivalent) for Active Directory, Exchange, Azure AD, Windows File Servers and Privilege Secure (PAM)		
		Real-time auditing of Active Directory (AD) changes, including user account modifications, group policy changes, and privilege escalations.		
		File server auditing to track file and folder access, modifications, deletions, and permission changes.		
		Automated alerts for suspicious activities, such as privilege abuse, unauthorized access.		
		Detect and respond to Active Directory attacks		
		Identify unmanaged, or unknown, privileged accounts with constant scanning. Stop attackers moving laterally in your environment by disabling unnecessary accounts.		

Monitoring, Detection, and Response				
Request #	Category	Product and Technical Specs Requested	Quantity Requested	Duration of Product/Service
MD&R 1	Penetration Testing	Penetration Testing (Pentest) & Vulnerability Assessments	1	One Time
		External and internal penetration testing to identify security gaps.		
		Regular vulnerability scans and risk assessments.		
		Wireless and network security scanning for vulnerabilities.		
		Remediation plans with prioritized risk-based recommendations.		
		Compliance validation for cybersecurity frameworks (NIST, CISA).		
		Comprehensive report with findings and mitigation strategies.		
MD&R 2	Vulnerability Scanning and Management Solution	Tenable (or equivalent) Vulnerability Scanning and Management	300	Annually - 3 Years Total
		Vulnerability scanning for servers, workstations, and applications.		
		Continuous asset discovery and risk prioritization.		
MD&R 3	Network Detection and Response (NDR) Solution	Capability to integration with SIEM, EDR, and patch management solutions.	300 Assetts (in 2 Sites)	One Time
		Darktrace (or equivalent) Network Detect and Response		
		AI-driven threat detection for network traffic anomalies.		
		Autonomous response to mitigate threats in real-time.		
		Lateral movement detection and data exfiltration monitoring.		
		Deep packet inspection (DPI) for advanced threat analysis.		
		Seamless integration with existing security infrastructure.		

Proposals should adequately address the following attributes for each category of service requested under this RFP, in addition to the required specifications of each request and category identifies in this RFP.

Endpoint Protection and Response

- Pre-Attack Surface Reduction, Breach Prevention AND Response and Remediation
 - Prevent full-blown data breaches before exfiltration can occur.
 - Proactive endpoint defense with pre-attack surface reduction capabilities based on advanced policy controls and technologies continuously scan for vulnerabilities and misconfigurations across applications, Active Directory, and devices.
 - Vulnerability Remediation
 - Breach Assessment
 - Contains device control which specifies block or allow policies on different types of devices that attach to client computers
 - App Isolation and App Control which allows known “good” applications to run, shields applications to prevent attackers from exploiting vulnerabilities and isolates unknown applications.
- Attack Prevention
 - Must immediately and effectively protect against file-based and fileless attack vectors and methods. Should implement machine learning and artificial intelligence use advanced device and cloud-based detection schemes to identify evolving threats across device types, operating systems, and applications.
 - Malware Prevention
 - Exploit prevention blocks memory-based zero-day exploits of vulnerabilities in popular software.
 - Should include prevention that enables fine-grained tuning of the level of detection and blocking separately to optimize protection and gain enhanced visibility into suspicious files.
 - Incorporates network connection security that identifies rouge wi-fi networks and delivers a policy-driven VPN to protect network connections and support compliance.

Identity Protection and Authentication

- Email Security – Spam Guard & Phishing Protection
 - Identifies and blocks spam, viruses and malware delivered via email messages.
 - Uses virus scanning, spam scoring, real-time intent analysis, URL link protection, reputation checks, and other techniques to scan email messages and files.
 - Stops advanced threats.
 - Blocks access to malicious URLs and attachments.
 - Protects data from corruption and deletion with full cloud backup and recovery of every email and file.
 - Keeps sensitive data safe with data leak prevention and encryption.

- Provides secure, tamper-proof cloud archiving of all incoming, outgoing, and internal emails to meet compliance, retention, and e-discovery requirements.
- Supports long-term retention policies, legal hold, and easy search and retrieval of cloud archived emails and attachments by authorized personnel.
- Active Directory, Email & File Server Auditing Solution
 - Secures your Active Directory from end to end, on premises and in the cloud, with a solution that addresses all the key functions of IT security: Identify, Protect, Detect, Respond and Recover.
 - Detects all changes in your Active Directory and Group Policy and provides the critical who, what, when and where details and before and after values.
 - Facilitates access control by reporting on both failed and successful attempts to log on to critical systems, as well as all ADFS logon attempts, and displaying the full logon history of any user.
 - Shows the current state of your users and groups, their permissions in Active Directory, your GPOs and their settings, and more, so you can easily compare them to a known good baseline.
 - Provides out-of-the-box reports aligned with controls from a wide range of standards, including PCI DSS, HIPAA, SOX, GDPR, GLBA, FISMA/NIST, CJIS and more.
 - Reports on changes to audit policy settings and other Group Policy modifications with full details and before and after values.
 - Enable data owners to approve permissions and access requests instead of burdening your IT team with the optional access reviews module.

Monitoring, Detection, and Response

- Penetration Testing
 - Identifies vulnerabilities in the current network environment and provides steps to address and mitigate.
 - Provides internal and external testing to identify security gaps for both wireless and hardwired network.
 - Provides a comprehensive report which documents findings and supports a framework for mitigation including strategy.
- Vulnerability Scanning and Management Solution
 - Provides around the clock vulnerability assessments.
 - Automates point-in-time assessments to identify software flaws, missing patches, malware and misconfigurations across a variety of operating systems, devices and applications.
 - Provides a variety of vulnerability scoring systems like CVSS v4, EPSS (or equivalent) to help implement effective vulnerability prioritization for remediation efforts.
 - Provides advisory and guidance on the next steps to take with a resource center that can guide experienced and non-security staff.
 - Contextualize threats, prioritize vulnerabilities, and optimizes response.

- Network Detection and Response (NDR) Solution
 - Identifies technologies and methodologies to detect and respond to suspicious activities and anomalies within network traffic.
 - Continuous monitoring of traffic patterns, identifying potential threats, and enabling swift response measures.
 - Uses techniques such as machine learning algorithms and behavioral analytics to analyze network traffic in real-time, which results in preventative and live threat detection, with targeted autonomous response to shut down and mitigate threat without disrupting school operations.
 - Uses AI automation.
 - Streamline incident response with AI automation, saving time and resources while ensuring minimal disruption to operations.
 - Provides detection, investigation, and response.
 - Identifies threat detection models and provides in depth comprehensive examples of the model(s) proposed.

[Remainder of this page intentionally left blank]

Proposal Requirements (Attachment A)

Proposals shall include, at a minimum, the following information organized as follows in a qualification statement:

1. A brief discussion of the consultant's/company's history, and services offered. Briefly state the Proposer understands of the work to be done and make a positive commitment to perform the work within the required time period.
2. Clearly state proposed fees and cost for services.
3. Resumes of key staff that will provide services and training.
4. Names and contact information of at five (preferably) client references in which you have been providing services for 5-10 years in the cybersecurity space. Clients in the field of educational technology are preferred.
5. Provide proof of CBE as firms certified as CBE will receive preferential consideration. See <http://dslbd.dc.gov/>
6. A proposed signed contract, which includes terms, payments and amount contract, will not to exceed.

[Remainder of this page intentionally left blank]

INSURANCE COVERAGE REQUIREMENTS (Attachment B)

General & Excess Liability Minimum Coverage

General Liability:	1,000,000
Umbrella Liability:	1,000,000

Company Name

Signature of Authorized Agent

Date Signed

FPCS will be named as additional insured on certificate of insurance if our firm or company is awarded a contract.

[Remainder of this page intentionally left blank]

Financial Statements (Attachment C)

Proposer should submit as Attachment C current financial statements, preferably for the past two years, which have been audited or reviewed by a Certified Public Accountant.

[Remainder of this page intentionally left blank]

Proposed Exceptions, Alterations, Additions, or Modifications to RFP (Attachment D)

Proposer should submit as Attachment D, any and all proposed exceptions, alterations, additions, or modifications.

For further information, contact Ruby Sherman at procurementinquiry@friendshipschools.org.

[Remainder of this page intentionally left blank]

ATTACHMENT E

CONFLICT OF INTREST DISCLOSURE

As a prospective vendor/supplier, its agents, employees, directors and/or assigns, you shall disclose any financial, business or other relationship with FPCS that may have an impact upon the outcome of this contract or potential future of the FPCS projects resulting from this effort. The prospective proposer, its agents, employees, directors and/or assigns shall also list current clients who may have a financial interest in the outcome of this contract or FPCS projects that will follow. In particular, the prospective proposer its agents, employees, directors and/or assigns shall disclose any financial interest or relationship with a member of the school's board or leadership.

Name of party that poses conflict

Relationship/Interest

Company Name

Signature of Authorized Agent

Date Signed

END OF FPCS RFP PACKAGE.