Request for Proposal 3092
For Procurement of
Data Center Firewalls
and
Accompanying Professional Services

RESPONSE TO THIS REQUEST FOR PROPOSAL IS DUE IN TO THE PURCHASING DEPARTMENT OF THE COMMUNITY COLLEGE OF ALLEGHENY COUNTY, 800 ALLEGHENY AVE., PITTSBURGH, PA 15233 NO LATER THAN:

May 26, 2017 AT 2:00 PM

Vendors must receive this RFP directly from the CCAC Purchasing Department. If received from another party, vendors must verify they are on the CCAC vendor list for this particular RFP. In so doing, bidders will receive all applicable addenda from CCAC. Failure to incorporate any addenda in the final submittal may result in the rejection of your proposal.

Interested parties may obtain further information from mcvetic@ccac.edu.

No fax or e-mail proposals will be accepted.
## Contents

1.0 PURPOSE 3

2.0 PROJECT BACKGROUND 3

- 2.1 CURRENT ENVIRONMENT 4
- 2.2 BUSINESS OBJECTIVES 4
- 2.3 SOLUTION VISION 5

3.0 SOLUTION REQUIREMENTS 6

- 3.1 FIREWALL REQUIREMENT 7
- 3.2 IMPLEMENTATION REQUIREMENTS 10
  - 3.2.1 Testing, Staging and Deployment Schedule 10
  - 3.2.2 Availability and Business Continuity 11
  - 3.2.3 Management and Monitoring 11
- 3.3 SECURITY AND AUDIT 11
- 3.4 TRAINING AND SUPPORT 11
  - 3.4.1 Training 11
  - 3.4.2 Support 11

4.0 SCHEDULE OF EVENTS 11

5.0 PRICING PAGE 23

6.0 APPENDIX A 24
1.0 PURPOSE

The purpose of this Request for Proposal (RFP) is to solicit proposals from qualified vendors for the procurement of enterprise data center firewalls that natively provide next generation high throughput intrusion detection & prevention (IDS/IPS), application control, micro segmentation and URL filtering capabilities and acquisition of professional services to install, configure, and integrate these solutions into the college networks for the Community College of Allegheny County. The RFP contains sufficient information and instructions to enable qualified bidders to prepare and submit proposals and supporting material. To be considered responsive, vendors must submit a complete bid that satisfies all requirements as stated in this RFP and its addendums. This RFP also contains all major terms and conditions that the successful vendor will be expected to accept.

The department of Information Technology Services (ITS) intends to implement the procured solutions starting in June 2017 and completed by July 2017.

**ONLY THE FOLLOWING MANUFACTURERS WILL BE CONSIDERED BY THE COLLEGE: CHECK POINT SOFTWARE TECHNOLOGIES, CISCO, FORTINET, OR PALO ALTO NETWORKS.**

2.0 PROJECT BACKGROUND

The Community College of Allegheny County is one of the largest institutions of post-secondary higher education in Pennsylvania. The college serves over 26,000 credit students through 170 degree and certificate programs and offers thousands of lifelong learning non-credit and workforce development courses to 35,000 students annually.

Incorporating a learning-centered environment committed to the future of the region, CCAC continues to expand its reach through innovative programming and accessible instruction offered via convenient day, evening, weekend and online courses. With four campuses and four centers serving Allegheny County and surrounding communities, CCAC endeavors to fulfill its mission to provide affordable access to quality education and offer a dynamic, diverse and supportive learning environment that prepares the region’s residents for academic, professional and personal success in our changing global society. More information about CCAC can be found at [https://www.ccac.edu/about/quickfacts/](https://www.ccac.edu/about/quickfacts/)

The next generation firewall solutions the college chooses through this RFP will be deployed at the college’s Network Operations Centers at the Office of College Services and South Campus disaster recovery site that are connected through a high speed network over a leased fiber from a service provider.

Therefore, the proposed systems must be scalable to the enterprise level with commensurate reliability. The college currently has approximately over 5000 managed endpoint and many unmanaged user owned Wi-Fi enabled handheld devices (i.e. laptops, phones, tablets, IP phones, smart phones, etc.). CCAC’s network infrastructure is managed by Network Services group in a centralized manner with strict adherence to well established guidelines.

The procured firewalls and management systems are expected to be rolled out as a greenfield systems (parallel system to the existing firewalls and network equipment) and the cut-overs to the new solution will be phased in to minimally impact college’s operations.

The new solution is expected to be completed by the end of July 2017. Since this time frame coincides with preparations for the start of the Fall Term, the vendor of the selected solution is required to work with the college IT staff to fully implement the chosen solution without impacting college operations.

*The college’s intention is to choose systems that provide best price/performance ratio and partner(s) that will meet the college’s requirements and demonstrate the ability to grow with us for many years to come.*
2.1 Current Environment
The college is currently utilizing network equipment manufactured by Cisco, HP, Dell, Palo Alto Networks, F5 Networks and Fortinet systems throughout the system. These systems include end user switches, core switches, wide area network optical equipment, routers, servers, SAN arrays, VPN gateways, firewalls, etc.

The college currently has approximately 5,000 managed computers (desktop, laptops, Windows Surface tablets), over 350 servers (physical and virtual) and over 200 network devices distributed through a high-speed wide-area network.

The majority of these desktop computers and servers are running Microsoft’s Windows operating systems. However, there are also some Linux based servers, Mac OSX clients and some operational technology equipment (building management systems, etc.).

Additionally, many unmanaged user owned Wi-Fi enabled handheld devices (i.e. laptops, phones, tablets, smart phones, etc.) can connect to the college’s network infrastructure through wired and wireless networks to access internet and college resources residing in the college’s main data center and at the disaster recovery site.

Currently, the majority of the college applications and services are located at the Office of College Services building however, there is a current college initiative to expand the disaster recovery capability of the college at one of the campuses. When this plan is materialized in the near future, some additional mission critical systems will also be located at this DR site.

The applications that are hosted in the primary date center are accessed by the college users from various college locations through internal wide area networks and Internet. However, the college systems are separated from Internet through a pair of institutional firewalls.

The network infrastructure and all mission critical IT services are centrally managed by the college staff at the Office of College Services building.

2.2 Business Objectives
In today’s information-driven business environment, dependency to the college systems, its data and underlying IT processes to deliver business outcomes is continuously increasing. The continuous availability and integrity of these IT systems is becoming a paramount necessity in order to stay operational and functional for the entire college.

Additionally, cloud based services, their integration & interoperation requirements and ongoing digital transformation of college business processes are creating significant information security risks and challenges for the institution.

These new game changing external forces are demanding in-house IT staff to change their long-established operational guidelines and practices to loosen these well-established information security practices in lieu of interoperability and immediate delivery of cloud based services to the institution.

The compounding effect of all these changes are negatively affecting the information security of the institution, bypassing change control measures and creating unmitigated risks for the college without proper information security controls implemented.

In order to address some of these issues, reduce the involved information security risks and secure the college’s information technology assets, the college is looking to acquire next generation high-performance data center firewalls to better protect and control the access to its most critical assets.

For this reason, the chosen firewall solution must provide greater intelligence and automation into information security operations to allow college staff to focus on what is most important, improving the college’s information security posture.
These planned high throughput, advanced data center firewalls are critical components of IT strategy. All services supported by the proposed data center firewall solution needs to be up and running 24 x 7 x 365. The selected firewall solution must enable or assist the college to achieve the following business objectives (the order of the list doesn’t reflect the importance or the priority of the objectives):

a. Support the College’s mission. Please see the https://www.ccac.edu/about/quickfacts/ for more information.
b. Improve the information security of the college’s most critical digital assets by protecting its data center, networks, applications and college data.
c. Drastically improve the information security posture of protected college assets without injecting transmission delay and impose significant operational complexity.
d. Improve network performance to accommodate current and future online learning experiences, like support of location agnostic high definition (HD) videoconferencing systems via multipurpose rooms to flexible personal systems and different form factor mobile devices.
e. Improve the college’s responsiveness to changing business conditions.
f. Improve network availability, resiliency and capacity without being cost prohibitive.
g. Granular, identity based enforcement of the college’s policies over new evasive, web based communication technologies (i.e. social media, web mail and popular remote access applications, P-2-P application sharing, etc.).
h. Gain deeper application visibility and control.
i. Improve malware protection and data loss prevention.
j. Facilitate PCI, FERPA, HIPPA compliance and reporting.
k. Seamless Integration with existing and planned security systems and tools.
l. Should have a centralized and effective management system which should enable the college to deploy, view and control all firewall activity through a single pane.
m. Must provide ability to automate routine tasks and drill-downs to produce maximum efficiency with minimal effort.

CCAC invites interested parties that meet the qualifications listed in this document to submit proposals regarding their product and related service offerings. All information shall be submitted in the format stipulated in this RFP.

2.3 Solution Vision
To secure its critical digital assets whether they are on the college premises or hosted on third party cloud based solutions, the college is seeking to acquire very high-throughput, non-blocking, redundant, application aware data center firewalls (hardware & software based) that offer effective intrusion detection & prevention services and micro-segmentation capabilities without affecting throughput, performance and capabilities of these firewalls.

These firewalls will protect the current data center hosts (physical and virtual) and future cloud based workloads that will host college digital assets and interoperate with on premises and other third-party cloud based systems.

In addition to this hardware based firewall solution that will be housed at the college data centers, the college is also seeking to implement a limited set of software based firewalls to protect its most critical Microsoft Hyper-V based virtual machines. Currently, all these systems are hosted on the college’s data centers.
However, some of these virtual machine workloads are expected to migrate to Microsoft and/or Amazon clouds over the next 3 to 5 years. When this migration is materialized, the college must be ready to provide same level of protection to these cloud hosted virtual machines independent of their location.

The selected vendor (or vendors) is/are expected to provide the following hardware, software, installation, configuration, testing, integration services and training:

a. The vendor of the selected firewall solution will setup and configure firewalls in high availability Active-Standby or Active-Active load-sharing and failsafe configuration to be determined by the college based on product HA support.

b. The vendor will configure the proposed new firewall solution to the college’s specifications fulfilling the requirements outlined this RFP, its addendums and subsequent project implementation meetings.

c. It is highly desired to have integration of web security gateway, and site to site IPsec VPN functionalities within the proposed firewall without impacting throughput requirements mentioned in this RFP.

d. The proposed firewall solutions that provide this level of integration out-of-box will be given higher priority and consideration.

The solution vision outlined above may evolve during the implementation period. All above configurations may require proposed systems to interface with existing core Cisco 6513 and HP 7510 switches. The selected vendor is required to study current core switch hardware and software network configurations for successful implementation.

In summary, the selected vendor (or group of vendors at college discretion) will provide the hardware installation, configuration, testing, migration, and eventual final configuration, software updates (if any), training, support and integration services for the proposed solution. The vendor will provide best practices for the optimal operation of their proposed solution.

Proposals that require computer hardware and server operating systems as part of their offering don’t need to cost out these components as a part of their proposal. These components will be procured by the college’s Information Technology Services. However, the vendors must provide their recommended specifications and optimal configurations, including memory, number and type of CPUs, disk space for the proposed system hardware and all the necessary software in their proposals. The college will separately procure the related necessary hardware to host any new management tool, as proposed by vendor.

The proposed solution will be purchased through the proper channels of CCAC procurement. Once a contract has been reached, a purchase order will be cut and development and implementation of the new solution will begin. The system will be rolled out in a phased approach as estimated in the project timeline prepared by vendor and approved by the college.

3.0 SOLUTION REQUIREMENTS

All work must be done under the supervision of a dedicated vendor’s most qualified certified networking expert (utilizing the resources of other less qualified technical personnel when it’s necessary and/or appropriate). The overall technical responsibility of the project is to be carried out by this dedicated/certified network engineer. At project completion, this dedicated engineer must provide and sign-off on the final document(s) to acknowledge the conformity of the work completed by the vendor.

The vendor must inventory all deliverables at the Office of College services with designated CCAC ITS staff person.
If the solution is awarded to multiple vendors, the vendors are responsible for their part of the project including the solution’s integration with the college’s network and coordination with other vendors working in parallel.

**Bidders are required to submit their responses as a comprehensive turnkey solution.** Therefore, all submittals must bundle the proposed designed products, vendor approved training, and technical labor, in addition to delineating material and labor in a clearly itemized list, as part of the vendor’s proposal. CCAC recognizes that this project involves significant technical capability for successful completion. Any information provided by CCAC with regard to this project is strictly confidential and shall not be disclosed to third parties.

The proposed solution(s) must satisfy the business objectives, solution vision, solution requirements and design objectives delineated herein. The vendor is solely responsible to deliver a fully functional solution meeting the specifications described in this RFP and its addendums.

After the award of the contract, the awarded vendor (contractor) is responsible for any necessary item not brought to the attention of CCAC before the award in order to complete the project by the specifications & design objectives.

### 3.1 Firewall Requirement

The college’s firewall security practice is to implicitly deny communications unless explicitly permitted. The data center firewall solution implemented should maintain at least “99.99%” availability. An Active/Active or Active/Standby solution is mandatory for high availability. The following requirements are mandatory. The data center firewall solution must:

- a. Support stateful protocol filtering, deep packet inspection, and detection of attacks within the payload.
- b. Provide advanced application identification and control.
- c. Support at least 100 Gbps sustained throughput with all firewall and associated security features enabled
- d. Per firewall, include a minimum of eight (8) 10 Gbps multi-mode fiber Ethernet interfaces, a minimum eight 100/1000 Mbps copper Ethernet interfaces, and a minimum of two 40Gbps Ethernet interfaces. All ports will be compatible and work with the existing network equipment.
- e. The proposed firewall solution must be extensible to accommodate the college’s growing needs and keep up with higher throughput requirements.
- f. Provide a modular hot swappable (1+1 redundant) dual power supply
- g. Support Active/Active and Active/Standby configuration modes for high availability.
- h. Must provide micro segmentation capability to block the lateral movement of nefarious network traffic in the data center networks.
- i. Must support Software Defined Networking (SDN).
- j. Must support dual stacking of IPv4 and IPv6 protocols for all firewall features and functions.
- k. If there is separate cost for licensing, this cost should be per device and should NOT be based on per user or IP endpoint (should support unlimited users).
The proposed firewall solution should provide fast (SSD), sufficient internal storage to retain the operational data on the device.

Must maintain user and application sessions when one of the high availability pairs (firewall devices) fails.

Provide secure access to diverse college applications that reside in the college data centers (i.e. Ellucian Colleague, SharePoint, SQL Server, VoIP, Exchange, Skype for Enterprise, streaming video, video conferencing, text messaging, Remote Desktop Services, web based line of business applications, etc.).

Enable secure remote access to the authorized resources from inside and outside of the college networks.

Must include integrated intrusion detection and prevention (IPS) function that offers advanced detection capabilities such as exploit signatures, protocol anomalies, application controls and behavior based detection.

IDS/IPS must be able to detect and prevent protocol misuse, malware communications, tunneling attempts and generic attack types without signatures.

IDS/IPS must detect and block unsanctioned peer to peer traffic.

Provide protection from zero day attacks and unknown threats.

Provide a centralized web management console and out of band Ethernet interface for management that supports SSHv2 and SCP.

Provide multiple security zones and interfaces to partition the data center networks into more manageable highly controlled network segments.

Must integrate with the college’s SIEM solution.

Ability to create granular security policy definitions per Microsoft Active Directory user and security groups to identify, block or limit usage of applications and widgets like instant messaging, social networking, video streaming, VoIP, games, etc.

Provide granular application function control to identify, allow, block or limit usage of applications and features within them.

Enable college staff to create detailed firewall security policies that is based on combination of multiple characteristics such as user’s identity, role in the college, computer name (NetBIOS name of the system is being used by the user) and specific aspects of an application.

Must seamlessly integrate with Active Directory to provide complete user identification and enable application based policy definition per user and/or group.

There should be advanced user and application controls such as ability to expand user groups, domain names as well as detailed user and application usage information in reports, logs and statistics.

Must offer adaptive real-time threat intelligence to improve firewall functions.
cc. The vendor must provide a three year product road map and all proposed systems and sub-components must be guaranteed not to be End-of-Life for at least five years.

dd. Hardware and software maintenance for each of the proposed solutions will be submitted for 24x7x4, 24x7xNBD, and 8x5xNBD.

ee. The proposed solution(s) must address the technical requirements and design objectives delineated herein. The vendor is solely responsible to deliver a fully functional solution meeting the specifications described herein. After the award of the contract, the awarded vendor (contractor) is responsible for any necessary item not brought to the attention of CCAC before the award in order to complete the project by the specifications & design objectives.

ff. The proposed solution must support automation and orchestration tool for policy application and future support for Network Function Virtualization (NFV)-attached virtual firewall to protect hypervisor managed configurations.

gg. The vendor must also offer a software firewall solution that works seamlessly with the physical hardware firewall to support future expansion. The software solution must work on the Microsoft Hyper-V hypervisor.

hh. The proposed solution must accommodate the placement of one firewall at the college’s main data center and the other one at the disaster recovery center at the south campus and configure these firewalls to operate in active/active or active/standby configuration (High-Availability Pair) depending on the solutions HA implementation to be decided by the college.

ii. Support all listed RFCs and standards at Appendix A: Firewall RFC/IEEE.

Desired Features

a. Firewall with integrated, web antivirus, antimalware/spyware, antivirus, antiphishing functionality, provided through a scalable and resilient platform that will not block high-throughput traffic

b. Granular, identity based enforcement of the college’s policies over new evasive, web based communication technologies (i.e. social media, web mail and popular remote access applications, P-2-P application sharing, etc.)

c. Dynamic policy-based network bandwidth control by application, user, source, destination, interface, IPsec VPN tunnel, URL categories, threats and data.

d. Integrated Web security gateway to protect from legacy, emerging/unknown, dynamic and scripted Web Malware. Web security gateway will help in controlling and mitigating security risks from network applications like instant messaging (IM) and peer–to-peer (P2P). Provide enhanced management and control, enabling real-time content analysis for both inbound and outbound web traffic and exhaustive PCI reporting.

e. Concurrent user software license for antivirus, antispyware functionality, URL filtering and blocking, antispam, antiphishing, and content filtering functionality, pattern file, and scan engine updates.
f. Ability to work with the college’s existing desktop and server antivirus solutions (SentinelOne), in addition to other third party antivirus vendors

g. Proposed solution may support agentless integration with Microsoft Active Directory and facilitate Microsoft AD user and group integration within the firewall security policy.

h. Proposed solution help prohibits the unauthorized transfer of files and sensitive data - like Personally Identifiable Information (PII), etc.

i. Support dual stacking of IPv4 and IPv6 protocols for all firewall features and functions in hardware

j. Capable of supporting two 100Gbps Ethernet interfaces per firewall

3.2 Implementation Requirements

The college expects the selected vendor to provide industry best practices for management of production services and any specifics related to their proposed solution. It is desired that the solution architecture is designed to accommodate future growth without requiring the college to invest in expensive network architecture redesign. In case the college chooses to work with more than one vendor for the right solution, it is expected that all vendors work together for the successful completion of the project. It is very important for vendors to understand the current network design and configuration and come up with a plan showing proposed solution steps. The following requirements are mandatory:

3.2.1 Testing, Staging and Deployment Schedule

a. Demonstrate prototype solution showing the configuration as it interoperates with the college’s network.

b. Describe how the solution works during link and device failure.

c. Vendors are required to submit the complete plan and action steps clearly specifying execution items.

d. The vendor is required to provide product road map and its end of life details.

e. The vendor must provide a summary of known outstanding bugs associated with the current network equipment image/software version.

f. The vendor must provide a physical and logical network diagram using Visio tool.

g. Vendors must work in such a manner that college business is not affected in any way. If emergency network down time is inevitable to deliver the proposed solution, at least 15 days prior written notice is required by the college’s ServiceDesk.

h. It is the vendor’s responsibility to install, configure and integrate the complete solution as per college business schedule.

i. One firewall of the high-availability pair will be placed in the main data center and the other one at the disaster recovery center at the south campus. These firewalls will be connected by a high speed optical network (a dedicated lambda) to sync all firewall configuration and data (including session information) for active/active configuration.
3.2.2 Availability and Business Continuity
The college’s information systems operate as a ‘virtual campus’, where users access these systems from any place at any time. The proposed design is expected to prevent possible single points of failure within the system.

3.2.3 Management and Monitoring
a. The vendor must specify the recommended and minimum memory, number of CPUs, and disk space for the proposed system hardware and operating system for the network management tool. The system must be installed and updated by ITS personnel on CCAC owned hardware located in the college’s network operations center.

b. Configure the management tool to provide alerts for failures via phone, text messaging, email etc.

c. Describe how the system logs errors, what error data constituents are documented and how to view useable information from log errors.

i. Describe any monitoring tools or plug-ins (i.e. Nagios plug-ins) that exists to monitor the system.

ii. Describe how the system monitors status.

3.3 Security and Audit
The solution should not cause security vulnerabilities.

3.4 Training and Support

3.4.1 Training

a. Provide manufacturer certified training for four CCAC employees to be trained to configure, operate and maintain the proposed solution. The assumptions about the proficiency of the CCAC personnel must be noted. CCAC may use these vouchers at any point in time.

b. Provide a list of the printed documentation provided for installation, operation, use, and administration of the whole solution.

b. Configure the management tool to provide alerts for failures via phone, text messaging, email etc.

c. Describe how the system logs errors, what error data constituents are documented and how to view useable information from log errors.

i. Describe any monitoring tools or plug-ins (i.e. Nagios plug-ins) that exists to monitor the system.

ii. Describe how the system monitors status.

3.4.2 Support

a. Describe if and how you will provide 24 x 7 support and the time frame of guaranteed initial response time.

i. Specify whether you will provide on-site support of initial installation.

ii. Describe other services for maintaining the solution in a supported state.

4.0 SCHEDULE OF EVENTS

RFP release ........................................................................................................................................... May 16, 2017
Close date for RFP questions ................................................................................................................ May 22, 2017
Proposal due 2:00 PM .......................................................................................................................... May 26, 2017
Contract signed (estimated) ..................................................................................................................... June 2, 2017
Implementation to begin (estimated) ........................................................................................................ June 5, 2017
All equipment and software must be received by .................................................................................. June 30, 2017
The project must be completed by .......................................................................................................... July 31, 2017
5.0 INSTRUCTIONS TO VENDORS

5.1 RFP Questions and Clarifications
Vendors shall aggregate their requests for clarification and submit them via e-mail to mcvetic@ccac.edu. Contact should be no later than May 22, 2017. Such requests for clarification, and CCAC's response, will be supplied in writing to all parties that have received copies of the RFP, without identifying the source of the inquiry.

5.2 RFP Response Format
Vendors must address all information specified by this RFP. All questions must be answered completely. CCAC reserves the right to verify any information contained in the vendor's RFP response, and to request additional information after the RFP response has been received. Any supplemental information that you provide must be in writing and will become part of your proposal.

Marketing brochures included as part of the main body of the bid response shall not be considered. Such material must be submitted only as attachments and must not be used as a substitute for written responses. In case of any conflict between the content in the attachments and a vendor's answers in the body of the proposal, the latter will prevail.

5.3 Cover Letter
The proposal must be accompanied by a covering letter, signed by an individual authorized to bind the proposed entity.

5.4 Vendor Profile and Demographics
Provide a statement giving a brief history of your company, how it is organized, and how its available products and resources will be used to meet CCAC's requirements and help achieve the business objectives stated above. The vendor shall submit the following information:

  d. The company's official name and address. The vendor shall also indicate what type of entity it is (i.e. a corporation or a partnership).
  e. The name, address and telephone number of the person who receives correspondence and who is authorized to make decisions or represent the vendor. Please state his or her capacity within the company.
  f. The total number of years the vendor has been in business and offering Solution products and, if applicable, the number of years under the present business name.
  g. The number of years that the vendor has been providing the specific Solution software and software that forms part of its current proposal.
  h. A description of the vendor's operations: facilities, business and objectives, and the number of employees.
5.5 Financial Information

Within 48 hours upon request by CCAC, the vendor shall provide a complete set of audited financial statements for the past three years. All financial statements should be prepared to generally accepted accounting principles. Each vendor should note that CCAC reserves the right to purchase credit reports and additional financial information as it deems necessary. The vendor shall also provide a copy of its corporate annual report.

5.6 Proposal Submission

Vendors' proposals should be mailed/delivered to the following address:

Michael Cvetic
Director of Purchasing
Community College of Allegheny County
800 Allegheny Avenue
Pittsburgh, PA 15233-1895

Please note that it is the vendor’s responsibility to ensure that the proposal and all other required documents are received at the address named above by the closing date specified above. CCAC will be the sole judge of the qualifications of all prospective candidates, and reserves the right to reject any and all submittals without recourse.

CCAC is aware that information contained in the proposals indicates the vendor’s current operations. Therefore, use of this information shall be confined to this request and will be treated as confidential.

Vendors shall bear all costs associated with preparing and submitting responses to this RFP and the subsequent evaluation phase. CCAC will, in no way, be responsible for these costs, regardless of the conduct or outcome of the prequalification process.

6.0 REQUIRED SUBMITTALS

The College requires that responses to this solicitation contain the following information:

SUBMITTAL FORM – 1: Vendor must complete, sign, and submit this page with their proposal response.

PRICING SUMMARY PAGES: Submit pricing pages (and attach detailed pricing breakdown).

REQUIRED DOCUMENTATION: Submit all documentation and support materials as described throughout this RFP.

REFERENCES – submit at least three customer references for similar services.

MBE/WBE PARTICIPATION: CCAC encourages the participation of minority and women-owned businesses in all of its contracts and is committed to providing maximum opportunities for qualified minority and/or women-owned business enterprises (“MBE/WBEs”) to participate in its work. Bidder agrees (1) if qualified, to take reasonable and timely steps to obtain appropriate certification as an MBE and/or WBE, (2) to ensure that MBE and/or WBEs are appropriately considered as subcontractors and/or suppliers under this Agreement; and (3) to report moneys spent for MBE and/or WBE subcontractors and/or suppliers for work as CCAC may from time to time reasonably request. CCAC’s goal for MBE/WBE participation is 15%. Please provide documentation as to your firm’s good faith effort to reach this goal by describing all applicable details of MBE/WBE participation that may be included in the resulting agreement.
7.0 GENERAL SUBMITTAL REQUIREMENTS

All proposal responses, inclusive of the required submittals and all other documentation, must be submitted in hard copy and either mailed, delivered by private carrier, or hand-delivered (no fax or electronic responses).

PROPOSAL DEADLINE: Proposals are due by 2:00 p.m. on May 26, 2017. (Proposals received late will not be considered by the College.)

One original and one digital copy (disk or flash drive) of such shall be appropriately identified and delivered to:
Community College of Allegheny County, Purchasing Department - Attn: Michael Cvetic, 800 Allegheny Avenue, Pittsburgh, PA 15233

Proposals shall clearly indicate company name, full address, contact person, phone number, fax number and e-mail address.

Proposals must contain the original signature of a duly authorized officer or agent of the company submitting the proposal.

Any/all information/language that is proposed to be incorporated into any final agreement shall be submitted with the vendor’s response.

All costs incurred in preparing a response shall be at the vendor’s expense

VENDOR REPRESENTATION / WARRANTY

Any responding vendor, by submitting a proposal, specifically represents and warrants that it has and shall possess, and that its employees, agents and subcontractors have and shall possess, the required education, knowledge, experience and character necessary to qualify them individually for the particular duties they perform. CCAC shall reserve the right to inspect and/or evaluate any potential awardee’s facility, physical equipment, staff, and all matters that may bear upon the ability to successfully perform the scope of work. CCAC shall conduct interviews of vendors as needed to evaluate qualifications. Should CCAC reasonably find that any vendor does not have the capacity to perform the work, CCAC may reject the vendor’s proposal.

8.0 GENERAL TERMS AND CONDITIONS

GENERAL TERMS AND CONDITIONS OF THE AWARDED CONTRACT

The following terms and conditions shall apply to any resulting contract. Any terms and conditions of a responding vendor’s that are in conflict with the College’s terms and conditions, inclusive of any specific contractual requirements, must be identified within the vendor’s response. CCAC may negotiate the inclusion, exclusion, or alteration of any language, terms, pricing or conditions prior to the issuance of a signed contract or throughout the term of the contract. The final contract shall incorporate the RFP document and any proposal submitted by the successful vendor and accepted by the College.
Additional phases of the project may be added at a later date beyond the initial award of the contract with the chosen vendor.

Vendors are cautioned that although the vendor’s terms may be submitted for consideration, the College reserves the right to negotiate its preference of the same, or otherwise reject the vendor’s proposal if the College is not able and willing to agree to the vendor’s terms.

**INVOICING/PAYMENT PROVISIONS:** The College’s payment terms shall be 30 days from the date the vendor’s invoice is properly presented and received. Invoices may be submitted only in accordance with deliverables that have been appropriately accepted by the College’s sign-off.

**TERMINATION PROVISIONS:**

a. The awarded contract may be terminated in whole or in part in writing by the College in the event of the failure by Contractor to fulfill its obligations under the terms and conditions of the contract, or in the event that the Contractor breaches any provision of the agreement (in the College’s opinion), provided that no such termination shall be effective unless Contractor is given three (3) calendar days' written notice of intent to terminate, delivered personally or by certified mail, return receipt requested, and an opportunity for consultation with the College prior to termination.

b. Upon receipt of a termination notice pursuant to the foregoing paragraph, Contractor shall promptly discontinue all services affected unless otherwise directed by the notice of termination.

c. Upon termination pursuant to the foregoing paragraphs, the College may take over the work and prosecute the same to completion by agreement with another party or otherwise. Should Contractor fail or refuse to comply fully and faithfully with the terms, conditions and stipulations of the resulting agreement, College shall have the right at their notion to cancel, annul and declare void the award and the contract without any liability whatsoever on the part of Contractor. The College shall be the sole judge as to whether or not Contractor has fully and faithfully complied therewith. College shall have the further right before or after any such cancellation to recover by law from Contractor any and all damages sustained by reason of non-compliance with or breach of the contract by Contractor.

d. Upon termination, an equitable adjustment of the fee shall be made, which shall not include any profit for services or other work performed. The Contractor acknowledges and agrees that it shall not be entitled nor shall it make a claim for lost profits or loss of anticipated earnings because of termination.

e. In addition to the College’s right to terminate as above stated, the College shall have the right to postpone, delay, or suspend or terminate the services for which Contractor is herein engaged at any time and for any reason deemed to be in the College's interest. In such event of suspension or termination for the College's convenience, the College shall pay Contractor for the services rendered through the date when notice of suspension/termination was received by Contractor. In the event of delay, postponement or suspension, Contractor agrees that it shall only be entitled to a reasonable extension of time to complete the project and not to monetary compensation.

f. CCAC shall also have the right to terminate any/all connections for any reason, at its own discretion, prior to the completion of the term. List early termination penalties on the bid sheet.

**INDEPENDENT CONTRACTOR STATUS:** It shall be expressly agreed that Contractor’s status hereunder an award is that of independent Contractor. Neither Contractor, nor any person hired by Contractor, shall be considered employees of the College for any purpose.
AUTHORITY TO BIND: In the performance of the awarded services, Contractor agrees that the Contractor shall not have the authority to enter into any contract or agreement to bind the College in any way and shall not represent to anyone that the Contractor has such authority.

GOVERNING LAWS: Any resulting agreement shall be governed by and construed in accordance with the laws of the Commonwealth of Pennsylvania.

EVALUATION AND AWARD OF PROPOSALS: While each proposal shall be considered objectively, CCAC reserves the right to accept or reject any proposal and to waive any formalities, informalities or technicalities in the RFP process at its own discretion.

CCAC will not be bound by oral explanations or instructions given by any CCAC employee or agent at anytime during the competitive proposal process or after award. Only modifications to specifications issued in writing by way of addendum shall be valid.

CCAC reserves the right to award this RFP in any manner that is determined to be in its best interest. The award may be split on a location-by-location basis, total low basis, or other basis.

The issuance of the College’s award letter and/or subsequent purchase order(s) shall constitute the award of any accepted proposal.

INSURANCE AND INDEMNIFICATION REQUIREMENTS: An insurance certificate as described on “Form B” (attached herein) must be submitted by the awarded vendor prior to any work being performed.

PERFORMANCE BOND REQUIREMENTS: SEE BELOW.

CONTRACTOR INTEGRITY PROVISIONS

The awarded Contractor must agree and abide by the following integrity, confidentiality and non-disclosure provisions:

COLLEGE’S INTERESTS: Contractor agrees that it will not during the term of the resulting agreement engage in any activity which is contrary to and in conflict with the best interests, goals and purposes of the College.

CONFIDENTIALITY: The Contractor shall not disclose to others any confidential information gained by virtue of the proposal process and the resulting contract.

COMPLIANCE WITH APPLICABLE LAW: The Contractor shall maintain the highest standards of integrity in the performance of the contract and shall take no action in violation of state or federal laws, regulations, or any other requirements that govern contracting with the College.

9.0 PURCHASE ORDER TERMS AND CONDITIONS

https://www.ccac.edu/Terms_and_Conditions.aspx
COMMUNITY COLLEGE OF ALLEGHENY COUNTY

INSURANCE AND INDEMNIFICATION REQUIREMENTS

FORM B

Indemnification. To the fullest extent permitted by law, Contractor shall defend, indemnify and hold harmless the Community College of Allegheny County (CCAC), its agents, officers, employees, and volunteers from and against all claims, damages, losses, and expenses (including but not limited to attorney fees and court costs) to the extent directly arising from the acts, errors, mistakes, omissions, work or service of Contractor, its agents, employees, or any tier of its subcontractors in the performance of this Contract. The amount and type of insurance coverage requirements of this Contract will in no way be construed as limiting the scope of indemnification in this Paragraph.

Insurance. Contractor shall maintain during the term of this Contract insurance policies described below issued by companies licensed in Pennsylvania with a current A.M. Best rating of A- or better. At the signing of this Contract, and prior to the commencement of any work, Contractor shall furnish the CCAC Purchasing Department with a Certificate of Insurance evidencing the required coverages, conditions, and limits required by this Contract at the following address: Community College of Allegheny County, Purchasing Department, 800 Allegheny Avenue, Pittsburgh, PA 15233.

The insurance policies, except Workers’ Compensation and Professional Liability, shall be endorsed to name Community College of Allegheny County, its agents, officers, employees, and volunteers as Additional Insureds with the following language or its equivalent:

Community College of Allegheny County, its agents, officers, employees, and volunteers are hereby named as additional insureds as their interest may appear.

All such Certificates shall provide a 30-day notice of cancellation. Renewal Certificates must be provided for any policies that expire during the term of this Contract. Certificate must specify whether coverage is written on an Occurrence or a Claims Made Policy form.

Insurance coverage required under this Contract is:

1) Commercial General Liability insurance with a limit of not less than $1,000,000 per occurrence for bodily injury, property damage, personal injury, products and completed operations, and blanket contractual coverage, including but not limited to the liability assumed under the indemnification provisions of this Contract.

2) Automobile Liability insurance with a combined single limit for bodily injury and property damage of not less than $1,000,000 each occurrence with respect to Contractor’s owned, hired, and non-owned vehicles.

3) Workers’ Compensation insurance with limits statutorily required by any Federal or State law and Employer’s Liability insurance of not less than $100,000 for each accident, $100,000 disease for each employee, and $500,000 disease policy limit.
11.0 PERFORMANCE BOND REQUIREMENTS

Performance Bond Required of Awarded Vendor – $25,000.00

Must use the college’s form on the next page.

In lieu of a performance bond, the awarded vendor may submit either a certified or cashier’s check or an Irrevocable Letter of Credit in the amount of $25,000.00.

Irrevocable Letter of Credit shall be as follows:

A contractor or supplier to the Community College of Allegheny County may substitute an Irrevocable Letter of Credit in lieu of a Performance Bond. If this option is chosen by the contractor or supplier, the Irrevocable Letter of Credit must include the following terms.

a. The terms of payment must be stated as follows:

“The drafts must be accompanied by your (CCAC) signed statement certifying that the contractor has not performed satisfactorily in accordance with the specifications and conditions of the contract. Unsatisfactory performance will be determined solely by the Community College of Allegheny County”.

b. The Irrevocable Letter of Credit must be payable and confirmed through a correspondent bank headquartered within the United States and which has total assets of at least $5 billion.

Any performance bond, certified/cashier’s check, or Irrevocable Letter of Credit submitted by the awarded vendor shall remain in effect (certified/cashier’s check held by CCAC) for a period of ninety days beyond the final date of acceptance and signoff by CCAC.
PERFORMANCE BOND

COMMUNITY COLLEGE OF ALLEGHENY COUNTY
800 Allegheny Avenue, Pittsburgh, Pennsylvania 15233

BOND NUMBER

PERFORMANCE BOND

Know all men by these Presents that we_____________________________________________________

(hereinafter called “Principal”) as Principal, and_____________________________________________________

authorized to do business in the Commonwealth of Pennsylvania (hereinafter called “Surety”) as Surety, are held and

firmly bound unto the Community College of Allegheny County, through its Board of

Trustees,_______________________

in the sum of_________________________

to be paid to the said College aforesaid, its certain attorney, or assigns. To which payment will and truly be made, said

principal and said surety to bind themselves, their respective successors or assigns jointly and severally, firmly by these

presents.

WITNESS our hands and seals, the ____________day of ________________________ the year of our Lord 2009.

WHEREAS the above bounded____________________________________________________________

has filed with the Community College of Allegheny County proposals for the________________

____________________________________The Condition of the above Obligation is such that if the

said____________________________shall perform_____________________________________________

In accordance with the agreement between____________________________________________________

and the Community College of Allegheny County of even date herewith and the specifications and proposals attached to

and made part of the agreement, shall indemnify and save harmless the said Community College of Allegheny County

from all liens, charges, demands, losses and damages of every kind and nature, whatsoever. Then this obligations to be

void, otherwise to be and remain in full force and virtue.

Attest: CONTRACTOR

(SEAL)

SECRETARY PRESIDENT Signed,

Sealed, and Delivered in presence of:
12. MASTER SERVICES AGREEMENT

THIS MASTER SERVICES AGREEMENT ("Agreement") is made and entered into as of this ____ day of ______________, 2017, by and between Community College of Allegheny County, with a business office located at 800 Allegheny Avenue, Pittsburgh, PA 15233 (hereinafter referred to as the “College”), and the company or business listed on the signature page hereto (hereinafter referred to as “Contractor”).

RECITALS

WHEREAS, the College has issued a Request for Quotation, Bid Solicitation, Request for Proposal, and/or a Purchase Order (hereinafter individually and collectively referred to as the “Order”), pursuant to Bid Proposal No.

which College seeks to procure certain work and services, as more fully described on the Order; and

WHEREAS, Contractor has submitted a proposal to the College to provide the services described in the Order, a copy of which is attached hereto as Exhibit A (hereinafter the “Proposal”) and incorporated by reference;

WHEREAS, the College desires to engage Contractor to provide the services, pursuant to and in accordance with the terms and conditions that this Agreement set forth herein.

NOW, THEREFORE, in consideration of the premises and covenants that this Agreement contains, the receipt and adequacy of which are hereby acknowledged, the parties, intending to be legally bound, agree as follows:

1. Term. The term of this Agreement shall be as specified in the Order unless otherwise stated in the section below. If no date is specified, this Agreement shall begin with the date first stated above and terminate upon satisfactory completion of the services described herein.

2. Services. Contractor shall fully and faithfully perform the work and services described in the Order and the Proposal and any specifications, scope of work or other documentation attached thereto. Contractor warrants that all work and services performed by or on behalf of it under this Agreement will conform to all terms and specifications set forth in the Order and in the Proposal.

3. Price/Fees: The College shall pay Contractor for the services and work performed by Contractor in accordance with the fees and/or prices set forth in the Proposal.

4. Terms and Conditions: This Agreement, and the services to be performed by Contractor hereunder, will be subject to and governed by College’s Standard Terms and Conditions for the Purchase of Goods and Services (“Master Terms”), which are incorporated herein by reference. The Master Terms can be viewed and downloaded at http://www.ccac.edu/default.aspx?id=149304. By signing below, Contractor acknowledges its receipt and acceptance of the Master Terms.

5. Insurance Requirements: In addition to the Master Terms, Contractor shall comply with the insurance and indemnification requirements set forth on Exhibit B, which are incorporated herein by reference. Prior to commencing performance of the Services, Contractor shall furnish to the College a properly executed certificate(s) of insurance which evidence all insurance required by Exhibit B. Said certificate(s) of insurance shall be attached herein as Exhibit C.
6. Assignment. Contractor may not assign or subcontract this Agreement or its performance thereof, in whole or in part, without the College’s prior written consent.

7. Entire Agreement; Modification. This Agreement, together with the Exhibits and other documents referenced and incorporated herein, sets forth the entire agreement of the parties on the subject matter hereof and supersedes all previous or concurrent agreements between them, whether oral or written. Any proposal, quotation, acknowledgment, confirmation or other writing submitted by Contractor to the College shall not be deemed to amend or modify this Agreement, and will be of no legal effect except to the extent that it serves to identify the work and services to be performed by the Contractor. This Agreement, and the terms set forth in the Master Terms, will control over any conflicting terms or provisions contained in any proposal, invoice or other documentation submitted by Contractor to College. The terms of this Agreement may not be modified or changed except by a writing that both parties sign. This Agreement shall inure to the benefit of the College and Contractor and the College’s successors and assigns.

IN WITNESS WHEREOF, the parties have executed this Agreement as of the day and year first above written.

CONTRACTOR:

By: __________________________
Signature: __________________________
Title: __________________________
Date: __________________________

COMMUNITY COLLEGE
OF ALLEGHENY COUNTY:

By: __________________________
Signature: __________________________
Title: __________________________
Date: __________________________

EXHIBITS - The following Exhibits are attached hereto and made a part of this Agreement for all purposes:

- Exhibit A - Contractor’s Proposal Response
- Exhibit B - Insurance Requirements
- Exhibit C - Contractor’s Certificate(s) of Insurance.
- Exhibit D – Performance Bond
13.0 SUBMITTAL FORM

By submitting a proposal the vendor acknowledges that following items are hereby understood and agreed to:

The undersigned, having carefully examined all sections and attachments to this Request for Proposal does hereby offer to furnish all labor, materials, equipment, supplies, insurance and bonds specified, and services necessary to fulfill the contract in accordance with the RFP which is/are hereby acknowledged by the signature below.

STATEMENT OF NON-COLLUSION

Finally, the undersigned also certifies that this proposal is made without previous understanding, agreement or connection with any person, firm, or corporation making a proposal on this same service and is in all respects, fair and without collusion or fraud.

SIGNATURE OF OFFEROR

(Must be signed by a duly authorized officer or agent of the responding company.)

Company Name:

Signed By:

Name (Printed):

FEIN: Title:

Address: Telephone:

Zip+Four: Fax:

Date: E-mail:
5.0 PRICING PAGE

PRICING PAGE – FIREWALL

In addition to this Pricing Summary Page, vendors must submit complete and itemized listings of all proposed charges (i.e.: equipment, parts, and materials; software, shipping; labor, installation, integration, and implementation; maintenance options; etc.). Systems proposed must be fully functional. The cost of any omissions will be the responsibility of the vendor.

<table>
<thead>
<tr>
<th>Description</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lump Sum Hardware Cost</td>
<td>$</td>
</tr>
<tr>
<td>Lump Sum Software Cost</td>
<td>$</td>
</tr>
<tr>
<td>Lump Sum Labor, Installation, Integration, Implementation, Testing, Training, and Other Costs</td>
<td>$</td>
</tr>
<tr>
<td>Grand Total</td>
<td>$</td>
</tr>
</tbody>
</table>

Hardware and Software Maintenance Options:

<table>
<thead>
<tr>
<th>Maintenance Option</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>24 x 7 x 4</td>
<td>$</td>
</tr>
<tr>
<td>24 x 7 x NBD</td>
<td>$</td>
</tr>
<tr>
<td>8 x 5 x NBD</td>
<td>$</td>
</tr>
</tbody>
</table>

Vendor Name: _____________________________________________________________
6.0 APPENDIX A

Appendix A: Firewall RFC/IEEE compliance requirements

Standards Compliance
1. IEEE 802.3 10Base-T
2. IEEE 802.3u 100Base-TX
3. IEEE 802.3u 100Base-FX
4. IEEE 802.3u 100Base-LX
5. IEEE 802.3z 1000Base-SX/LX
6. IEEE 802.3ab 1000Base-T
7. IEEE 802.3ae 10-Gigabit Ethernet
8. IEEE 802.3ad Link Aggregation
9. IEEE 802.1q VLAN Tagging

RFC Compliance - BGPv4
1. RFC 4271 BGPv4

RFC Compliance - OSPF
1. RFC 2328 OSPF v2

RFC Compliance - IPv6 Core
1. RFC 2460 IPv6 Specification

Quality of Service
1. RFC 2475 An Architecture for Differentiated Services

Security Options
1. Stateful firewall with ACL filters
2. Content filtering
3. DoS, DDoS, Anti-Replay,
4. Antivirus, anti-spam, IPS
5. Policy based control
6. IPsec VPN with encryption (3DES- 168 bit & AES – 256-bit) and authentication (MD-5 and SHA-1)
7. IPsec NAT traversal

Management and Control
1. SNMP v2c/v3 MIB-II with traps
2. Web-based Graphical User Interface with reporting tool
3. Industry Standard Command Line Interface (CLI)
4. Secure Shell (SSHv2)
5. Secure Copy (SCP)
6. Syslog