Request for Proposal 3091

for Procurement of

Security Information and Event Management (SIEM) Solution

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 12 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.

1.0 PURPOSE

The purpose of this Request for Proposal (RFP) is to solicit proposals from qualified vendors for the procurement of Security Information and Event Management (SIEM) system and the acquisition of professional services to install, configure, and integrate the solution with other college systems.

This Request for Proposal (RFP) will require the vendor to provide all relevant information about the completed installation in both printed and digital formats. The vendor will provide an operation & maintenance (O&M) manual that will cover all components and systems in a way that is easily understood. The college is not interested in acquiring managed services and/or a hosted solution at this time.

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 May 2017 and completed by August 2017.

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 30,000 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/

The Security Information and Event Management (SIEM) solution the college chooses through this RFP will be deployed at the Office of College Services Building at 800 Allegheny Avenue, Pittsburgh. However, the implemented system will collect information from multitude of college equipment and data sources located at other college locations throughout Allegheny and Washington Counties in addition to cloud based systems. For this reason, the proposed solution is expected to be a two-tier or multi-tier solution that includes centralized log management (CLM) that is separate from the SIEM functionality in order to provide needed scalability and redundancy and cost effectiveness.

These remote data sources communicate with the selected SIEM solution over the college's wide area network and Internet.Therefore, the proposed solution must be scalable, highly secured and resilient to the enterprise level with commensurate reliability.

The new solution is expected to be completed by the end of August 2017. Since this time frame coincides with 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 college. These systems include end user switches, core switches, wide area network optical equipment, routers, servers, SAN arrays, VPN gateways, firewalls, printers and tape libraries.

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 wide-area network.

Most 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.) that need to be integrated into the chosen SIEM solution in phases over time.

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.

There are well over 20 applications that may expose operational logs. These logging sources may need to be monitored, data collected, correlated and analyzed through the selected solution where the college sees it necessary or required.

Currently, most of these college applications 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 hence these systems need to be monitored through the procured SIEM solution.

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

The information security function at the college has only one dedicated FTE to manage and support the InfoSec operations. However, some members of the infrastructure and server operations groups handle the information security related matters when the information security related issues overlap with these groups' workloads.

2.2 Business Objectives

In today's information-driven business environment, college systems and processes capture an ever-increasing amount of data. To derive meaningful and actionable information from this captured operational data and improve information security, the college is looking to acquire a two-tier or multi-tier security information and event management system (SIEM) that offers:

1. A centralized log management (CLM) component (tier-1) to improve foundational information security capabilities of the college and provide scalability and redundancy for log collection and management functions of the system.
2. An advanced analytical SIEM component (tier-2) to provide high-performance advanced threat detection, near-real-time event processing and correlation, historical data analysis, and the integration of contextual and threat intelligence data. This component also must include compliance and incident reporting, automated alerting of common security events, historical analysis for detected incidents and interoperate with other college information security systems using industry standard protocols.

While all business areas of the college are impacted to varying degrees by digital transformation and consumerization of information technology over recent years, few departments in the college face a greater challenge than the information technology services department and specifically the information security.

To support its mission to protect the college's critical information assets, the information technology services department must maintain a diligent, continuous processes to monitor, capture, correlate, analyze, transform and subsequently act on the information collected from a wide array of systems across the institution.

During this ingestion process, the collected vast amount of data must be quickly analyzed, actionable information extracted and acted on in near real-time which will place even greater demands on the Information Technology Services department's already strained workforce.

For this reason, the chosen security information and event management (SIEM) 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.

In this context, the selected solution is expected to:

1. Automate the data collection, normalization, correlation, transformation and analysis functions to establish security baselines
2. Identify potential information security issues that are too complex and may not be visible to human eye.
3. Interoperate with other college information security systems to participate in the mitigation of identified issues by automating actions based on gathered intelligence to improve the information security posture of the college.
4. Able to ingest multiple user identity data stores (Active Directory, application database accounts, non-Windows based account, etc.) into the SIEM, have it correlated, analyzed and use it to discover end user usage patterns that can be further used to identify anomalies.

The college expects the selected solution to ingest data from and fully interoperate with the college systems that identified in appendix A in order to deliver the proposed benefits and achieve all the objectives stated in this RFP.

In the end, the utilized technology solution must enhance the college's information security posture, improve information security effectiveness and deliver best price / performance ratio to in order to be sustainable over its lifecycle.

The chosen solution must enable or assist the college to achieve the following business objectives (the order of the list doesn't reflect the importance or priority of the objectives):

a. Streamline compliance reporting (i.e. PCI DSS 3.2, FERPA, HIPPA, etc.) and keep up with the changing compliance regulations.
b. Provide effective real-time monitoring, incident detection and response capabilities that contributes to automated incident handling workflows.
c. Improve efficiency of incident handling activities by providing workflow/case management capability to assign phases of incident to specific team members with pre-established deadlines and reminders with optional acknowledgements.
d. Able to algorithmically analyze multiple sources of information in order to flag potential breaches and interoperate with other security tools to contain those incidents.
e. Reduce the number of false positives by first ensuring that the discovered event has been felt by other college systems before triggering an action/alert by holistically correlating and analyzing data, etc.
f. Provide a range of tools and functionalities to facilitate the management of security-related events, minimizing reducing by assessing log data and correlating information coming from various sources.
g. Provide capability to automatically respond to detected attacks and breaches that are still in progress and work with other security tools to contain compromised hosts.
h. Allows an incident handler to quickly identify an attack's route through the institution with ease.
i. Enable college staff to rapidly identify all hosts and/or users that were affected by a particular attack, malware, malicious act, etc.
j. Improve network and business application security posture without injecting transmission delay and significant operational complexity.
k. Able to easily adapt to changing college business practices to provide responsive and effective information security services when such need is arise.
l. Improve the college's information security posture, systems availability and resiliency without being cost prohibitive.
m. Provide deeper insight into college operations, identify dark data, systems utilizations and end user usage patterns through analysis of collected data and take an action based on predetermined rules defined by the college.
n. Improve malware protection and data loss prevention by working with the college's endpoint protection and other information security tool vendors.

o. Being able to store actionable data for at least 365 days.
p. Provide capability to manually and automatically export the collected data into regular formats (.csv, .txt, .log, XML, JSON, etc.) for long-term archival/backup.
q. Be able to store 2 years of historical data that can be exported to other systems for further processing and analysis and long-term pattern discovery.

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

The college (CCAC) is seeking to acquire a multi-tier advanced SIEM solution to improve its information security operations. The procured SIEM solution must be scalable, easy to manage and reconfigure, fault tolerant (hardware and software) and cost effective in order to achieve the objectives mentioned in this RFP and its subsequent addendums.

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 solution will install & mount, setup, configure and integrate the proposed solution with the identified systems, test and confirm the interoperability of the design.
b. The vendor will setup, configure and integrate the proposed SIEM solution to the college's objectives and specifications and fulfil the requirements published in this RFP.
c. The vendor will provide all relevant information (design, as-built configuration, disaster recovery information, etc.) for the installed solution. The provided information should be formatted to work in Microsoft Word and Excel.
d. The vendor will provide an operation & maintenance (O&M) manual that will cover all components and systems in a way that is easily understood.
e. The vendor will perform knowledge transfer of all programming to ensure CCAC can provide ongoing maintenance for installed equipment.
f. The vendor will provide sufficient training credits (for either online or premises based training) for 5 ITS staff to adequately operate the proposed solution.

The solution vision outlined above may evolve during the implementation period. All above configurations will require proposed systems to interface with existing college systems. The selected vendor is required to study current environment (switch hardware and software configurations) and for successful implementation.

In summary, the selected vendor (or group of vendors at college discretion) will provide the hardware installation, configuration, testing, and configuration, software updates (if any), training, support and integration services for the 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 that is prepared by vendor as part of its proposal.

3.0 SOLUTION REQUIREMENTS

Hardware and software maintenance for each of the proposed solutions will be submitted for 24x7x4, 24x7xNBD, and 8x5xNBD. Additionally, the college requires vendors to submit a table showing the total cost of ownership over a 6-year time period. Please see Page 23 for the format of this table and required information for determining the total cost of ownership for the proposed equipment.

All work must be done under the supervision of the vendor's most qualified, dedicated and 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 a 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 address business objectives (defined in section 2.2), solution vision (defined in section 2.3) and all the requirements and design objectives delineated herein. The vendor is solely responsible to deliver a fully functional solution meeting the specifications described herein. If the vendor regards the technical specifications as insufficiently exacting, he will offer equipment that will achieve the collective goals at their cost.

Functional requirements apply before specific technical requirements, and the overall system requirements apply before the requirements for single components. 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 SIEM Functional and Technical Requirements

The proposed SIEM solution will collect data from many network equipment (Cisco, HP, Aruba, F5, Palo Alto, Fortinet and Dell, Microsoft etc.), Web based applications (Blackboard LMS, IIS, Apache Tomcat, etc.), database servers (MS SQL, MySQL, etc.), application servers (Exchange, Skype for Business, etc.), file and print servers, AD domain controllers, DHCP Servers, WINS Servers.

The majority of these systems are hosted in the college's main network operations center at the Office of College Services Building however, some systems are located at other college locations.

Additionally, the proposed solution will collect data from operational technology equipment, building environmental control and management systems that reside at different locations throughout the college.

For this distributed nature of the college operations, the proposed solution should be secure, high performance, scalable to handle required current and future workloads and be resilient for hardware and network related failures.

The proposed solution must meet the following mandatory requirements:

a) Collect, parse, normalize, categorize, and store data from wide variety of college systems (i.e. servers, applications, network infrastructure, building management systems, cloud based application, etc.)

b) Must be able to sift through, analyze, operate, report on at least 8 terabytes of annual collected data without creating performance, capacity or response related issues.

c) Correlate and analyze data; detect cyber threats in as close to real-time as possible

d) Must be able to consume external, cloud based threat intelligence feeds and use this information to detect threats, speed-up breach detection and accelerate response.

e) The proposed design is expected to prevent possible single points of failure within the system. Provide redundancy without being cost prohibitive.

f) Able to assist in performing forensic analysis to determine the root cause of the operational problems and security incidents.

g) Provide security analytics to assist in the analysis of the impact and/or scope of a potential information security incident

h) Expose relationships between physical and virtual machines, network infrastructure, business processes and data, and present the risks and threats in context to provide real-time threat intelligence

i) Improve efficiency of incident handling activities by providing workflow/case management capability to assign phases of incident to team members with deadlines and optional reminders

j) Allows an incident handler to quickly identify an attack's route through the institution

k) Provide flexible and resilient deployment options for scalable and non-service or performance impacting log collection

l) Accelerate the discovery and qualification of information security threats

m) Improve the college's information security posture by providing 24x7 monitoring and participate in automated intelligent response

n) Streamline audits and compliance reporting processes (i.e. PCI DSS 3.2, FERPA, HIPPA, GLBA, etc.)

o) Being able to detect external attacks, data exfiltration attempts and internal misuse in their tracks and interoperate with other information security components to stop these threats

p) Provide user and entity behavior analytics (UEBA) capabilities to detect anomalous user activities (i.e., an external attacker who has breached the college's perimeter defenses and compromised an internal host and a user's credentials, and is using those credentials to move laterally through the college).

q) Utilizing user and entity behavior analytics (UEBA) to reduce the college's information security related risks by detecting prohibited or unauthorized activities by trusted insiders, such as employees, contractors and external third parties.

r) Provide out-of-the-box reporting templates for a broad range of regulatory frameworks (FERPA, PCI DSS 3.2, HIPPA, CIS Top 20, etc.)

s) Ingest and analyze NetFlow and other flow based data (i.e. sFlow) from the college's existing routers and switches to deliver complete, real-time visibility into all hosts and traffic on the network, providing actionable insight for addressing a wide variety of network and security issues.

t) The proposed SIEM solution must support industry standard threat information exchange languages/protocols such as "Structured Threat Information eXpression" (STIX) and "Trusted Automated Exchange of Indicator Information" (TAXII) in order to rapidly add and configure diverse threat intelligence from commercial or open-source feeds and also exchange information with other internal college information security tools.

u) Provide operational insight for optimization of information security related workflows

v) Increase information security operational efficiency and expedite incident management processes

w) Must produce useful information and spit-out actionable data in a reasonable amount of time in order for the college staff to make informed decisions

x) Provide a solution that is easy-to-deploy and maintain, scalable and highly affordable to acquire and run over the lifetime of the proposed solution

y) Provide granular, role-based dashboards (security trimmed) and automated daily reports for authorized staff to review the findings and confirm the integrity of the systems that they are responsible for. Additionally, provide overall system health information to all members of the information security team regardless of their role in the operation of the proposed solution.

z) Present system's findings and analytics in a clear and logical manner to save staff time in review of information security reports and findings

aa) Lessen the amount of time and expertise required to adequately monitor and manage the volumes of log data and information that are collected through the college

bb) Provide capability to perform root cause analysis of information security related events in real-time with built-in intelligence

cc) Eliminate false positives from true positives and alert responsible college staff only those events that are relevant in real-time when an anomaly or threat is detected (through SMS, email, etc.) and interoperate with other information security tools (i.e. firewalls, IPS, etc.) to immediately contain the identified threats at network speed

dd) Provide role-based access security to the system's components, findings and analytics for the college's IT teams to make sure that only authorized staff will have access to the collected information

ee) Maintain a detailed logging functionality for the proposed system to retain all system communications, system and user activities, and other critical system information that is pertinent for secure system operations

ff) Provide ample growth capacity for compute and storage to add more systems to monitor and collect data from

gg) Retain the collected actionable data for at least 12 months

hh) Must provide adequate redundancy for hardware and connections without being cost prohibitive if a hardware based solution is proposed

ii) Lower the long term operational costs

jj) Provide at least 4 wire-speed auto-MDIX, 100/1000 Mbps copper Ethernet ports if a hardware based solution is proposed

kk) Support hot swappable redundant power supply and fan (For physical appliances)

ll) Must offer auditable, granular control over systems changes, individual users, applications and virtual machines

mm) Must support SSHv2 and Secure Web for remote management using TLS 1.2.

nn) Support SNMP version 3.0

oo) Be a modular, scalable, industry standards-based platform and must interoperate with multi-vendor devices and management tools without losing its stated features essential for compliance with this RFP

pp) 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

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

rr) 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

3.2 SIEM Desired Features

a. Provide capabilities for real-time monitoring, user behavior baselining, data and user monitoring, application monitoring for threat management and compliance

b. Provide advanced contextual-security analytics utilizing user and entity behavior analytics (UEBA) and external threat intelligence.

c. Capability to collect logs and other pertinent system information from the monitored systems without installing agent on source systems

d. Provide capability to baseline information security patterns; detect and differentiate between activity patterns that can be good indicators of normal as well as abnormal activity.

e. Able to log data analysis is intended, in part, to help you differentiate between normal and abnormal behavior.

f. Provide high availability and resiliency

g. Provide at least 2 wire-speed 10 Gigabit Ethernet ports for full packet capture of network traffic.

h. Daily bandwidth usage monitoring

i. Provide ticketing and workflow capability to improve the information security operations through process automation and capture intermediate process steps along each workflow

j. Retain the collected actionable data for 2 years for on-demand search and historical reporting

k. All proposed equipment and software must be IPv6 compliant and must be enabled in the provided configuration

3.3 Implementation Requirements

The college expects the selected vendor to provide industry best practices to the college's staff for the ongoing management of proposed system and any specifics related to the operation of the proposed solution. It is desired that the solution architecture is designed to accommodate future growth without requiring the college to invest in expensive forklift replacement and 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:

3.3.1 Testing, Staging and Deployment Schedule

a. Demonstrate the functional production solution showing the configuration as it communicates and collect data from the identified college systems. This will showing the operational effectiveness of the proposed solution that just installed/implemented with minimal configuration effort (out of box).

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

c. Vendors are required to submit a complete project plan with details and action steps clearly specifying execution items.

d. The vendors are required to provide the type and level of support that they expect from the college to complete their work as proposed.

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

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

g. The vendor must provide a physical and logical network diagram using Visio tool detailing IP addresses, device name, image versions, link aggregation port assignments and trunk port assignments.

h. 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.

i. Since most SIEM integration related workloads involve changing of equipment configurations such as configuring logging destinations, vendors are required to identify the project workloads that would require an outage of other college equipment as part of this project.

j. It is the vendor's responsibility to install, configure and integrate the complete solution as per college business schedule and on time.

3.3.2 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.

3.3.3 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 exist to monitor the system.

   ii. Describe how the system monitors status.

3.4 Security and Audit

As a principle, the proposed solution should not cause any security vulnerability to the college systems.

a) Vendor must provide information about their responsible disclosure program/process.
b) Vendor should provide procedures for patching of the proposed solution including the third party components that the proposed solution relies on.
c) List all third-party software that is necessary for the operation of the solution and will require down time of the proposed SIEM solution during patching.

3.5 Training and Support

3.5.1 Training

a. Provide manufacturer certified training for 5 CCAC employees to be trained to configure, operate and maintain the proposed solutions and any college requested technology. 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 digital documents for installation, operation, use, and administration of the whole solution. These documents must be structured, editable, portable, and searchable. All major sections of the content of these documents must be identified within the beginning of each document.
c. In addition to vendor's official product support, if it is available, the vendor is expected to provide full access to its online forums/user community for the identified college staff to get support from their peers from other institutions.
d. In addition to formal classroom training, the college requires the vendor to provide on-site training of key concepts which are specific to the proposed solution. The vendor must specify the type of training provided.
e. Specify and describe any help files provided by the system, and whether they can be customized for CCAC.

3.5.2 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 what type of work is expected from the college staff in order to implement the proposed SIEM solution. Please provide other services for maintaining the solution in a supported state.

4.0 SCHEDULE OF EVENTS

RFP release	**May 2 2017**
Close date for RFP questions	**May 9 2017**
Proposal due 2:00 PM	**May 12 2017**
Vendor demonstrations (as needed).	**May 15 2017**
Contract signed (estimated)	**May 24 2017**
First project meeting (estimated)	**Week of May 29 2017**
The project is completed on (estimated)	**August 10 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 9, 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 Friday, May 12, 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 College. 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

(For Awardee Only)

10.0 INSURANCE AND INDEMNIFICATION REQUIREMENTS

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.

(For Awardee Only)

11.0 PERFORMANCE BOND REQUIRMENTS

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.

(For Awardee Only)

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:

(For Awardee Only)

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: 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:

Request for Proposal 3091

for Procurement of

Security Information and Event Management (SIEM) Solution

and Accompanying Professional Services

PRICING PAGE

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.

Lump Sum Hardware Cost	**$**
Lump Sum Software Cost	**$**
Lump Sum Labor, Installation, Integration, Implementation, Testing, Training, and Other Costs	**$**
Grand Total	**$**

Annual Hardware and Software Maintenance Options (pricing to be held firm for at least three years):

24 x 7 x 4	**$**
24 x 7 x NBD	**$**
8 x 5 x NBD	**$**

Vendor Name: ____

Appendix A: Listing of college systems

Vendor	Model/Application	Quantity
Apache	Tomcat Application Server	6
Apache	Apache Web server	10
Aruba Networks	Aruba Wireless LAN controllers	13
Aruba Networks	Aruba Clearpass	2
Box.com	Cloud Storage	10
Brocade	SAN Switch	8
CentOS / Other Linux	Linux	32
Cisco	IOS based Routers and Switches	175
Cisco	Call Manager	2
Cisco	Unity Connection	1
Cisco	IronPort Mail Gateway	2
Cisco	MDS Storage Switch	2
Dell	Dell Hardware on Intel-based Servers	63
Dell	Compellent Storage	4
F5 Networks	Local Traffic Manager	2
F5 Networks	Web Accelerator	2
Fortinet	FortiGate firewalls	4
Fortinet	FortiManager	2
HP	HP/3Com Comware Switches and Routers	10
IBM	DB2 Database Server	3
Data Air	HVAC	3
Liebert	FPC	2
Liebert	UPS	3
Microsoft	Windows 2000, Windows 2003, Windows 2008, Windows 2008 R2,	333
Microsoft	DHCP Server - 2003, 2008, 2012	9
Microsoft	DNS Server - 2003, 2008, 2012	13
Microsoft	Domain Controller / Active Directory - 2003, 2008, 2012	13
Microsoft	SQL Server - 2005, 2008, 2008R2, 2012, 2014	25
Microsoft	IIS versions	116
Microsoft	ASP.NET	30
Microsoft	HyperV Hypervisor	213
Microsoft	DFS Servers	11
Microsoft	Sharepoint Server	6
Microsoft	ADFS	4
Microsoft	Exchange Server	5
Nessus	Vulnerability Scanner	1
Palo Alto Networks	PAN-OS based Firewall	9
Qualys	Vulnerability Scanner	1
Redhat	Linux	5
VMware	VMware ESX and VCenter	1
SentinelOne	SentinelOne Management Console hosted on Amazon S3	1