PURCHASING DEPARTMENT
6600 34TH AVENUE
MOLINE, IL 61265

DATE: August 20, 2019

TO BE OPENED ON
September 3, 2019
RFP 01-20 *Addendum 1*

IMPORTANT
SHOW **"RFP 01-20 *Addendum 1*"** ON OUTSIDE OF MAILING ENVELOPE

REQUEST FOR PROPOSAL (RFP)
IT AUDIT
RFP 01-20 ADDENDUM 1

Pursuant to the provisions of Section 3-27.1 of the Illinois Public Community College Act and rules and regulations adopted thereunder, sealed proposals subject to the conditions and requirements made a part hereof **will be received until 2:00 p.m. local time, on Tuesday, September 3, 2019, in the Finance Office at Black Hawk College Quad Cities Campus, located at 6600 34th Avenue in Building One, Second Floor, Room 244A, then opened publicly, read aloud and recorded immediately thereafter when possible, in the Black Hawk Room, Room 255,** for furnishing the goods or services described below, to be delivered or performed at the location(s) stated. Whether or not a proposal is timely shall be determined by reference to the clock located in the Purchasing Office of the College, and the determination of whether or not a proposal is timely in accordance with that clock shall be at the sole discretion of the Black Hawk College Purchasing Office and Board of Trustees, whose decision on that issue shall be final.

REFER INQUIRIES TO:	**MIKE MELEG** **BLACK HAWK COLLEGE** **6600 34th AVENUE** **MOLINE IL 61265**
TELEPHONE:	**(309) 796-5002**
EMAIL ADDRESS:	**melegm@bhc.edu**

VENDOR INFORMATION:
Contact:
Company:
Address:
City/State/Zip:
Telephone:
Fax Number:
Email Address:

GENERAL

Proposals are subject to the attached Standard Terms and Conditions (Attachment A).

USING DEPARTMENT

IT Department

Here are the questions received, in order, by the deadline of 5:00 pm August 16, 2019, and their answers:

Q: How many IP addresses to perform the Penetration Testing?

A: Page 4 of the RFP
Subnets: Scan all subnets externally available to the Internet.
2Class C's – QC Campus. QC has a redundant internet connection. 1 Class C per ISP.
15 addresses only in a Class C – East Campus
68 address at Quad City campus

Q: Whether we need to take care of the application installation (antivirus) and or College will cover this?

A: No installation. This is a review of our current systems. Symantec Endpoint protection is the AV. Cisco Firepower Threat Defense is the IDS/IPS. We are looking for a review of these systems not a replacement.

Q: Do we also need to help the College in implementing the controls (technical controls) which will be identified during the gap assessment?

A: Provide deficiencies between current BHC practices and best practices. Rate them and make recommendation on how to get to best practices. The college is implementing it.

Q: External -180 IP's - need to confirm if these are active...we only scan active.

A: Approximately 83

Q: How many web apps total?

A: 10 -40

Q: How many employees would be included in the email phishing exercise? We would typically do about 3 different emails for 1 campaign over time period agreed upon.

A: Approximately 524

Q: Typically, our telephone social engineering is 6 – 8 calls. By then we pretty much know how your employees are trained. Is that reasonable?

A: 8 to 10 would be acceptable

Q: Maybe I missed this, but work will be awarded 9/27/19. Is there a timeframe when you expect the work to be performed?

A: Starting October running through December, with some social testing in the early spring 2020.

PROJECT SCOPE

Q: There is a mention of “Brute Force Attack” in the project scope. What would be the target of this brute force attack? Active directory, web application, FTP server, etc.?

A: It would be the bookstore controller which are Windows server and workstations, Active directory, web application, FTP server, Banner, Recruit

IT General Controls Review

Q: Is there more detail around what is being requested in the Internal Security Controls? Is this an objective review of current procedures against best practices?

A: Yes

Q: What is the deliverable from the review of these procedures?

A: Provide deficiencies between current BHC practices and best practices. Rate them and make recommendation on how to get to best practices.

Q: Will the controls review be based solely on documentation review or are interviews desired to better understand the risk tolerance/security objectives of the organization?

A: Interviews as well as documentation review.

Q: In the section “Access privileges for Microsoft Active Directory,” what specifically is being audited? User permissions? Protocols and authentication, Group Policies, DNS security, etc.

A: A review of all AD privileged groups need to be reviewed for account memberships

Q: What is the current antivirus and IDS/IPS products in place? Is this a review of these systems or are you looking for recommendations for replacements?

A: Symantec Endpoint protection is the AV. Cisco Firepower Threat Defense is the IDS/IPS. We are looking for a review of these systems not a replacement.

Information System Policies

Q: What is the specific objective deliverable in the policy review? Is this to review and edit existing policies for gaps against best practices?

A: Yes. Rate them and make recommendation on how to get to best practices.

Q: Should new policies be proposed for replacement?

A: Yes, if any policies are missing rate them and make recommendations.

Perimeter Penetration Testing

Q: Internet Perimeter testing is understood. Can more detail be given about the wireless network testing? How many SSIDs are in scope for the test? What types of authentication are in place – WPA2-PSK, WPA2 Enterprise? Testing for WPA2 Enterprise may include a rouge AP and would require some coordination.

A: 3 SSIDS. WPA2 Enterprise & WPA2 PSK. No exclude a rouge AP at this time.

Internal Security Scan

Q: What is the objective of the internal testing? Are the servers listed the only systems in scope or are there workstations that would be included as well?

A: All servers, random samples of desktops, AV equipment, UPS and printers.

Q: Active Directory testing often requires some interaction with workstations to determine vulnerabilities for example.

A: We can work this out at the time of test.

Q: What is the total number of servers that should be in scope? The listing includes Physical Servers and Virtual Servers but does provide a quantity.

A: Between 100 – 150

Q: What is the level of effort desired for internal testing? Vulnerability scan or penetration testing? Should there be proof of exploit provided for vulnerabilities that are identified for example?

A: Penetration testing. Exploit should be listed along with remediation steps.

Bookstore

Q: Is there more information around the scope for the requirement “Attempt to gain access to POS systems from external and any internal BHC network.”? This may require exploitation and could scale to social engineering as well. What should be the level of effort and attack strategies approved for this requirement?

A: Brute force attack on the bookstore systems along with social engineering for bookstore employees.

General Pricing Information

Q: Pricing is being requested for each section independently. Will the final bid be all inclusive or is there a desire to choose ala-carte pricing?

A: The goal is all inclusive but depending on cost ala-carte might be needed.

Q: Will Black Hawk College consider modifications to the RFP, including the Standard Terms and Conditions, which would be typical for the industry and type of services contemplated? Such modification requests would include, but not necessarily be limited to, modification of insurance provisions based on the way our policies apply; warranty and remedy provisions typical for the type of services contemplated; indemnification obligations limited to third party claims; inclusion of a provision limiting our total liability, except for our indemnification obligations, to an amount equal to the fees we receive under the executed Agreement, and exclude indirect, consequential, exemplary or similar such damages. Such requested modifications would be included as exceptions included within our proposal.

A: Black Hawk College will not consider modifications to the RFP because the Request for Proposal seeks bids based on the College’s needs and expectations, including but not limited to the Standard Terms and Conditions, insurance requirements, warranty and remedy provisions, indemnification, liability, etc. Such requested modifications could be included as exceptions within a proposal.

Q: Will the Business Continuity Plan be in place prior to this assessment?

A: No

Q: Is cyber Incident Response included in the BCP scope as well?

A: No but it would be in the IT Audit under general controls.

Q: Is wireless penetration testing in scope?

A: Yes

Q: If so, how many access points and buildings/locations are in scope?

A: 3 SSID's would need to be tested to see what can be accessed from each ID.

Social Engineering

Q: How many employees does the college have to include in the scope of the phishing email?

A: Approximately 524

External Perimeter Penetration Testing

Q: Of the externally facing subnets, can you confirm if the number of devices/ hosts are accessible within those ranges?

A: Page 4 of the RFP **Subnets:** Scan all subnets externally available to the Internet.
2Class C's – QC Campus. QC has a redundant internet connection. 1 Class C per ISP.
15 addresses only in a Class C – East Campus
68 address at Quad City campus

Q: Are there any web applications in scope of testing?

A: Yes

Q: If so, please provide the URL's and a summary of the applications.

A: URL's will be provided to RFP winner. 10-40

Internal Security Scans

Q: Are you requesting a limited scope test of only the domain controllers and virtualization platform?

A: No there will be over 100 servers including the domain controllers and virtualization platform.

Q: How many workstations are on the college and book store networks?

A: 7 at the bookstore, all servers, random samples of desktops, AV equipment, UPS and printers.

Q: Is internal penetration testing in scope?

A: Yes

Q: Is the bookstore on the same network as the college?

A: It rides a layer 2 Vlan landing on a DMZ interface of the firewall.

Q: Is this testing required to meet PCI (Payment card industry) requirements?

A: Yes for the bookstore

Q: How many expected presentations will be needed where the RFP noted “Vendor must be available to present a summary of the audit to the BHC BOT Cyber Security subcommittee and BHC Board of Trustees at designated meetings”? Two or more?

A: 3 to 4 different meetings with one of them being the BOT.

Q: How many users and security groups does the College currently have?

A: 5161 Users and 589 Groups

Q: Are servers managed by one central group or decentralize and managed by departments?

A: Over 100 servers by one central group

Q: How many locations are in scope?

A: 7

Q: Approximately how many policies and procedures exist?

A: 5 - 10

Q: How many employees does the College have?

A: Approximately 524

Q: Do you want to know how each employee responds to each different type of email phishing as noted in the RFP?

A: Yes

Please be reminded of the following:

10. ACKNOWLEDGEMENTS OF ADDENDA

Signature of company official on original document shall be construed as acknowledgment of receipt of any and all addenda pertaining to this specific proposal. Identification by number of addenda and date issued should be noted on all proposals submitted.