

Midwestern Higher Education Compact

Security Scanning & Audit and Related Services Request for Proposal Security Scanning & Audit

A.	Introduction.....	1
B.	The Midwestern Higher Education Compact.....	1
C.	The Midwestern Higher Education Compact Technologies Committee	2
D.	Security Scanning & Audit Solution.....	2
E.	Eligible Participants.....	4
F.	The MHEC RFP Process	5
G.	The Request for Proposal (RFP)	5
1.	<i>General Information and Qualifications</i>	5
H.	Functional Specifications Of Security Scanning & Audit	8
1.	<i>General Product Specifications and Guidelines</i>	8
2.	<i>Specifications</i>	9
3.	<i>Training</i>	12
4.	<i>Maintenance</i>	12
I.	Pricing.....	13
1.	<i>Price/Fee Increases</i>	14
2.	<i>Certification of Independent Price Determination</i>	14
J.	Signatory Authority.....	14
K.	Conflict of Interest.....	14
L.	RFP Development Process	14
1.	<i>Schedule of Events</i>	14
M.	Pre-proposal Conference and Requests for Clarification	15
N.	Submission Deadlines and Format	16
O.	Selection of Finalists and Best and Final Offers From Finalists	16
P.	Provider Selection	16
Q.	Contract Term.....	17
R.	Incurring Costs	18
S.	Method of Operation.....	18
T.	Analysis of Information.....	18
U.	Contacting MHEC.....	18

A. Introduction

The Security Products Committee of the Midwestern Higher Education Compact's Information Technologies Taskforce is requesting proposals from vendors on behalf of the Midwestern Higher Education Compact. The purpose of this Request For Proposal is to establish a comprehensive Security Scanning & Audit solution for the Eligible Participants in the 12 state region of the Compact. At a minimum this solution will offer competitive price agreements with qualified vendor(s) who shall provide hardware and/or software, support services, training and related materials and or services in accordance with the specifications of this Request For Proposal.

B. The Midwestern Higher Education Compact

The Midwestern Higher Education Compact (MHEC) is an instrumentality of twelve Midwestern states (Illinois, Indiana, Iowa, Kansas, Michigan, Minnesota, Missouri, Nebraska, North Dakota, Ohio, South Dakota, and Wisconsin). The Compact was established in 1991 through a common statute enacted into law by each of the member states. The purpose of the Compact is to promote higher education through interstate cooperation and resource sharing.

A 60 member Commission composed of five delegates from each state who are appointed by their respective Governors, House Speakers and Senate Presidents governs the Compact. The Commission has been conferred very broad authority to enact solutions and enter into agreements on behalf of its member states. Once a state enacts the necessary legislation to become a member of the Compact, all of the public and private non-profit colleges, universities, community colleges and technical colleges in the state are eligible to participate in the solutions established by the Compact. The Commission receives its primary financial support from member state appropriations, from foundations having special interests in specific solutions, and from administrative service fees.

The primary constituents served by the Midwestern Higher Education Compact are the approximately 1000 public and private non-profit institutions in the member states whose combined enrollments total over 4 million students. In addition, where appropriate, state government agencies and local school districts are also invited to participate in MHEC solutions. Faculty, staff, and students may also be eligible to purchase under a MHEC agreement, depending on the terms negotiated.

One of the Compact's top priorities is to establish public-private relationships to improve services to higher education, and reduce administrative costs for both providers and institutions. Since 1992, the Compact has engaged in several highly successful initiatives in cooperation with leading corporations. These relationships have been quite innovative, and have produced financial benefits for *all* of the involved parties. Beyond excellent pricing and terms, MHEC agreements deliver a primary benefit to institutions *and vendors* by avoiding the time and expense of the RFP process since MHEC has already completed the RFP and awarded the contract on behalf of all institutions in the twelve states.

C. The Midwestern Higher Education Compact Technologies Committee

In 1992, the Commission established the MHEC Telecommunications Committee to develop innovative approaches to expand access to telecommunications services, while reducing costs to institutions. Similarly, in 1999 the Commission established a Computing Resources Taskforce to identify opportunities to improve access to computing products and services and to reduce administrative costs. Both the Telecommunications Committee and the Computing Resources Taskforce were able to develop successful solutions that benefited higher education, K-12 schools and state and local governments. In January 2003, MHEC convened a joint meeting of these two committees. Since emerging technologies are blending into both the computer and telecommunications areas, the two 12-state committees were joined together and renamed the MHEC Technologies Committee. From this larger committee, smaller working group committees continue to focus on specific solution initiatives. As one, the Security Products Committee is responsible for developing this RFP.

The Commission believes that the services and scalability of the initiative envisioned by the Security Products Committee will offer unique advantages and benefits to private sector partners and to participating colleges and universities that cannot be readily achieved through individual actions. Mega-group participation will enable significant streamlining of marketing, administration and service functions; improved service support and training options; and operational efficiency across a variety of Eligible Participants and their individual scenarios. In order for this solution to be successful, it must be profitable for both the providers and the institutions. The Commission is committed to making that happen.

D. Security Scanning & Audit Solution

The MHEC Security Products Committee intends to provide a Security Scanning & Audit solution for Eligible Participants, collectively known as SIEM, and comprised of the following two components:

SEM (Security Event Management) – the monitoring of event data from network-connected equipment, and the software running thereunder to provide event recording, analysis, and notification in real time.

SIM (Security Information Management) – the collection, reporting and analysis of log data to monitor resource usage, threat management, and perhaps for regulatory compliance.

In addition to the applicable hardware and/or software, any proposed solution needs to have as options, the maintenance, technical support, training, and professional services necessary to allow the institution to fully utilize the solution. Because institutions have differing needs, the solution must be flexible enough to meet those varying needs. Amongst different types of institutions, and even within a single institution, differences in requirements exist. Therefore, the solution should allow adaptation to the specific needs and circumstances of each Eligible Participant as well as streamline and simplify the procurement and distribution process for them.

Furthermore, respondents are encouraged to offer innovative solutions, recognizing that to compete effectively they need to deal with a range of institutions: some will search for a rock bottom price because they have sufficient internal resources and expertise to provide their own pre- and post- sales support and servicing; whereas other institutions (perhaps having no technology support staff whatsoever) may need complete support. Some institutions will be willing to buy exclusively from one vendor; others will not. Some institutions will be willing to standardize purchases, do bulk buys, or provide local warranty services, while others will be unable to do so. Each of these factors provides the vendor an opportunity to show initiative and ultimately cement a long-term relationship with specific institutions.

The successful respondent(s) will be responsible for delivery of all hardware and/or software awarded. Respondents may propose the use of servicing subcontractors or resellers. However, MHEC will consider the respondent(s) to be the sole point of contact with regard to contractual matters, including pricing structure, delivery, warranty, and payment of any and all charges resulting from the purchase of products specified in this proposal, unless a separate contract addendum to the master price agreement is executed with said subcontractors or resellers.

If subcontractors or resellers are utilized, MHEC encourages the consideration of minority owned and/or economically disadvantaged businesses.

It is MHEC's belief that it has a successful history of creating renewable and reviewable purchasing vehicles for its institutions, and that its ability to foster relationships with vendors puts it in a unique position to bring the best value to all involved. It is our hope that by means of this RFP we will establish a purchasing vehicle for our eligible participants that will:

1. Represent enough volume that the pricing is aggressive enough to make this the most attractive purchasing vehicle available to our institutions
2. Use that volume to provide vendors with a more predictable business model so that they may reliably invest in providing those services that establish relationships and to reestablish in our institutions the value of value-added services so that vendors also have a more predictable space in which to market advanced fee-based services.
3. Allow MHEC to bring its educational, collaboration, and communications capabilities to bear in assisting vendors to build relationship with our smaller institutions without incurring substantial cost.

MHEC is seeking vendors and manufacturers who are willing to work with MHEC to provide creative solutions that will be effective within the confines of the purchasing regulations to which member institutions are bound.

The Security Scanning & Audit Solution will be offered to eligible institutions. The solution will:

1. Be designed as a renewable multiple-year offering capable of serving the entire MHEC region;
2. Offer Eligible Participants a streamlined and simplified procurement process that meets their Security Scanning & Audit needs;
3. Make available a comprehensive Security Scanning & Audit solution that is flexible enough to adapt to the specific needs and circumstances of each Eligible Participant;
4. Offer the highest quality Security Scanning & Audit products;
5. To avoid repeated RFPs from Eligible Participants (testing the market), clearly provides the best pricing structures in the region;
6. Assist Eligible Participants in the conversion, installation, training and support of the hardware and/or software as necessary;
7. Enable Eligible Participants, consortia of institutions, and systems currently under separate contract with the selected vendor(s) to convert to the MHEC Security Scanning & Audit Solution;
8. Be structured to enable institutions, consortia of institutions, and systems in MHEC member states to participate as they deem appropriate and in their own best interests;
9. Offer the selected vendor(s) the opportunity to deal with groups of Eligible Participants in unique ways, facilitated by MHEC.
10. Offer the selected vendor(s) opportunities to address the MHEC Commission on topics of mutual interest.

Depending upon the responses received and the solutions presented, the Security Products Committee may select more than one vendor to work with in developing and implementing SEIM solutions.

E. Eligible Participants

All public and private non-profit colleges, universities, community colleges, technical colleges and higher education agencies in MHEC member states shall be eligible to participate in the MHEC Security Scanning and Audit solution.

Optionally, participation may be negotiated by any or all of the following groups:

- K-12 schools and districts, including public libraries;
- cities, counties, hospitals, and local subdivisions;
- state agencies;
- faculty, staff, and students for any or all of the above groups

Contract benefits may differ for each of these optional groups.

MHEC will also entertain proposals to expand this solution to states within the other three Compacts in the country; WICHE, SREB, NEBHE, subject to their approval.

F. The MHEC RFP Process

This RFP is issued by the Midwestern Higher Education Compact's Security Products Committee. The person responsible for managing the procurement process is Mr. Grant Crawford (612) 626-6383 or grantc@mhec.org who is the sole point of contact for the Committee during the RFP process

The purpose of the RFP is to provide interested parties with information to enable them to prepare and submit a proposal to provide comprehensive solution(s) under the auspices of the Midwestern Higher Education Compact. MHEC has determined that developing a region-wide Security Scanning & Audit acquisition strategy through one or more providers will benefit both the higher education community and the provider(s). The Committee intends to use the results of this process to enter into a Master Price Agreement(s) to make the solutions available to the entire constituency of the Compact. Consequently, it will afford providers a truly competitive opportunity to advance product sales and services and to further penetrate a specific market niche.

G. The Request for Proposal (RFP)

In preparing responses to this RFP, prospective providers are asked to address

- the following questions pertaining to the manner in which they would envision the development of the solution;
- the strategies that they would employ to assure the solution's success; and
- the qualifications and unique features that they would bring to the solution.

As used in this RFP, the terms "must", "shall", "should" and "may" identify the criticality of requirements. "Must" and "shall" identify requirements whose absence will have a major negative impact on the suitability of the proposed solution. Items labeled as "should" or "may" are highly desirable, although their absence will not have as large an impact and as requirements labeled as "must" or "shall". Depending on the overall response to the RFP, some individual "must" and "shall" items may not be fully satisfied, but it is the intent to satisfy most, if not all, "must" and "shall" requirements. The inability of a Respondent to satisfy a "must" or "shall" requirement does not automatically remove that Respondent from consideration; however, it may seriously affect the overall rating of the Respondent's proposal.

1. General Information and Qualifications

1. The successful contractor(s) shall provide the enterprise hardware and/or software, maintenance, installation, training and service solution as described in this RFP. Respondents shall completely review the requirements specified in this request for proposal. It shall be the respondent's responsibility to make certain that all hardware, software, and support is included in their proposal to guarantee a fully functional enterprise Security Scanning & Audit system. It shall be the contractor's responsibility to verify that any software proposed will work as specified with the other proposed products.
2. The successful contractor must warranty all hardware and/or software and ensure that this product works to its maximum capacity for a minimum period of twelve (12) months after final acceptance by the Eligible Participant that purchased it.

3. The successful contractor must agree that additional products relative to obtaining the solution not covered herein may be added by an Eligible Participant to this contract without voiding provisions of the existing contract. The successful contractor with additional consideration may be allowed to furnish additional products and services to institutions covered within the MHEC region.
4. The bidder's order fulfillment process shall be considered an important process with regards to the existing business practices of Eligible Participants. Invoices must be received separately for campus business units. The Contractor's order fulfillment system must work seamlessly in conjunction with common ERP systems and/or member institutions purchasing card systems that Eligible Participants may choose to use.
5. Performance of the successful contractor(s) will be closely monitored by an oversight committee for the Master Price Agreement throughout the contract period. Individual institutions have the ability to control their own ordering process under the contract's Master Price Agreement. If deliveries prove to be unsatisfactory, or other problems arise, MHEC reserves the right to delete product or services from the Master Price Agreement and/or cancel Master Price Agreement for cause, and may award to the next acceptable respondent, or cancel and request new proposals. Similarly, if deliveries prove to be unsatisfactory or other problems arise under the agreement for an Eligible Participant, the Eligible Participant retains all of its remedies for a default. Failure of the Eligible Participant to exercise its rights of termination for cause or other remedies for default due to a respondent's failure to perform as required in any instance shall not constitute a waiver of termination rights or other default remedies in any other instance.
6. Delivery of purchases will be made within 30 calendar days after receipt of order, F.O.B. destination (interior/ground floor or inside dock), and freight pre-paid and allowed, to any and all locations of the Eligible Participant. Bid prices must include all packing, freight, insurance charges and installation/operation manuals.
7. Contractor agrees to notify the Eligible Participant within five working days after receipt of the order if they are unable to deliver within the required time frame. Failure of the contractor to adhere to delivery schedules as specified or to promptly replace defective product shall render the contractor liable for all costs in excess of the contract price when alternate procurement is necessary. Respondents need note that all locations of any particular Eligible Participant may not be within the MHEC region.
8. As some Eligible Participants have locations outside North America, contractors must also provide expected delivery times outside of North America.
9. Purchase orders will be placed by each Eligible Participant, on their institution's Purchase Order Form or by using a credit card on the vendor-supplied purchasing web site.
10. Contractors may choose to deliver products electronically where practicable. This option must be under the independent control of each Eligible Participant.
11. Contractor(s) must not substitute any item(s) that has been ordered by the Eligible Participant using this contract without the prior written or electronic approval by the

appropriate purchasing officer of the Eligible Participant. The substitute item must be at the same or better technology level than the original product ordered, and pricing at the same or lower price. Failure to comply may result in return of merchandise at contractor's expense.

12. Successful contractor(s) must offer a "total satisfaction" return policy. The contractor must provide a thirty (30) day no-questions-asked return option, from the date of delivery to end-user.
13. Successful contractor(s) shall be responsible for replacing at no cost to Eligible Participants any damaged or inoperable-on-receipt products received under this contract within 30 days from notification by that institution. This includes all shipping costs for returning non-functional items to the contractor for replacement.
14. Any price reductions from manufacturer from the time of submission of a purchase order to product delivery must be passed on to the Eligible Participant that issued the purchase order.
15. Successful contractor(s) shall retain and maintain all records and documents relating to this Contract for six years after final payment by the Eligible Participant hereunder or any applicable statute of limitations, whichever is longer, and shall make them available for inspection and audit by authorized representatives of the Eligible Participant, including the procurement officer or designee, at all reasonable times.
16. MHEC reserves the right, but is not obligated, to request that each respondent provide a formal presentation of its proposal at a date, time and place to be determined. If required by the MHEC Security Products Committee, it is anticipated that such presentation will not exceed two (2) hours. No respondent will be entitled to be present during, or otherwise receive any information regarding, any other presentation of any other respondent.
17. MHEC reserves the right to require a Financial Capacity report consisting of the following:
 - a. Sources of financing (shareholders, venture capital, etc.)
 - b. Bank references and name of auditing firm
 - c. Last two annual reports and all quarterly reports since the last annual report
 - d. Identification of the Parent Corporation and any subsidiaries
 - e. List of all current customers in the MHEC region, and all customers for whom similar work was performed during the past 2 years.
18. Successful contractor(s) must provide an account executive/team for MHEC. This team must establish and maintain fundamental familiarity/understanding with MHEC and MHEC's Eligible Participants. The account team must be able to recommend appropriate hardware, software, and support products based on their knowledge of that specific Eligible Participant.
19. Respondents wishing to offer services must do so in at least eight of our member states. For service to be considered offered in a state it must be offered in the *whole* state.
20. MHEC has incurred, and will continue to incur, costs and expenses in the development, implementation, administration and marketing of this program. To help recover some of these costs, the Technologies Committee requires an administration fee in this program. Please include an administration fee component in your proposal. The Respondent will be responsible for the administration fee. The administration fee

may be a flat rate, or it may be a variable rate based on volume. However, it is important to remember that regardless of the makeup of the administration fee, the overall pricing must remain extremely competitive for Eligible Participants.

21. Contractor must indicate country of manufacture and country of assembly.
22. Increasingly, Eligible Participants are committed to promote environmentally sound procurement, usage and disposal methods which are in compliance with State, County, and Municipal regulations. Many Eligible Participants have a recycling program for starch and Styrofoam packing peanuts. Our preference is to receive starch peanuts whenever possible. The Contractor shall not use INSTAPAK™ or mix starch and Styrofoam peanuts under any circumstances. Each product shall be separately pre-packed in accordance with commercially accepted methods. Small products may be packaged in protective envelopes (Mail-Lite or Bubble-Jet packs).

H. Functional Specifications Of Security Scanning & Audit

1. General Product Specifications and Guidelines

While MHEC recognizes that utilization of proprietary methods or protocols sometimes provides competitive advantage, MHEC will give preference to those vendors whose products support open source or also support recognized industry standard methods and protocols.

All products should be offered in **current production** as of the date of the award. Hardware components shall be new. ***For purpose of this contract “current production” shall mean that all equipment including the overall solution is being manufactured as new for the United States market.***

Refurbished equipment is not acceptable.

All solutions ordered with a hardware component as stated in the RFP must be shipped with that hardware fully configured with the required memory, components, and selected or specified operating system.

MHEC entities operate a managed environment with a stable managed lifecycle:

- Vendors should describe the product upgrade schedules and historical frequency of upgrades.
- Vendors should describe the compatibility between current and previous versions of their products
- Vendors shall provide their product road map(s) for all solutions proposed.
- Vendors shall indicate which third-party software packages are required for their application to function correctly (for example, operating systems, Web servers, databases, agents or clients for backup), and they should indicate who is responsible (the customer or the vendor) for purchasing and maintaining licenses for these packages.
- Vendors shall describe the timeframe that agents for their solution are available following the release of a new version of an operating system (for example, how long after Windows 2008 R2 Server was released, did your agent support Windows 2008 R2 Server)

Please provide a general description of the proposed SIEM solution that also defines how your SIEM deployment objectives and requirements will be met in each of the following areas:

- Information capture
- Log management and data archiving
- Security event management (real-time monitoring)
- Incident management
- User and resource access monitoring
- Reporting

2. Specifications

General

1. list all data collectors
2. list all collectable data elements
3. Vendors must ensure that all aspects of their solution are secure to unauthorized access. Please describe how proposed solutions maintain this security, including any application interfaces.
4. The vendor must provide a checklist of implementation steps that the vendor follows and/or that the customer must follow to ensure the security of the environment.

Architecture

1. Describe the components that compose your product's architecture, and indicate how each component is packaged (software, appliance, virtual appliance, as a service, etc.).
2. Indicate the operating systems the server side of your solution runs on.
3. Describe the recommended or standard base size of a typical deployment (i.e., how many devices are supported by a standard deployment)
4. Describe how the SIEM architecture "scales" from small colleges to state-wide implementations.
5. Describe how the SIEM architecture supports deployment in highly distributed environments.
6. Describe how your SIEM functions are integrated with other solutions that you provide.

Administration

1. Support for centralized administration in a geographically dispersed deployment.
2. Support for role-based access and delegated administration.
3. Integration with Active Directory or other repositories for role and resource groupings.

Information Capture

1. Describe information capture capabilities, and include a general description of available methods (system log, agent, application programming interface [API]).
2. Support for reduction, filtering and bandwidth management of the collected data.

3. Describe capabilities and user interfaces to collect and parse data from sources not formally supported.

Log and Data Management

1. Supported database management systems (DBMSs) for SIEM event data.
2. Do you provide compressed online information store for event or log data? If yes, indicate compression ratio in response.
3. Describe specific support for the collection storage and management of all log data from every source.
4. Describe integration of the log management component with other SIEM components (if it's a discrete component).
5. Forward filtered subset of log data in native format from the log management tier.
6. Indicate and describe support for data archiving and restoration of event and log data.
7. Describe capabilities/process for preserving the digital chain of custody.

Security Event Management (SEM): Real-Time Event Management and

1. Indicate support for real-time correlation. Describe capabilities in comments, including tiered deployment (across log manager or server instances).
2. Indicate support for an event taxonomy. Describe support for normalizing events from multiple sources.
3. Indicate the number of predefined correlation rules.
4. Indicate support for a correlation-rule-authoring system.
5. Indicate support for other real-time-event analysis methods. Provide details in comments.

Incident Management

1. Indicate native support for incident management workflow.
2. List problem management systems with which you have integration capabilities, and describe integration (e.g., e-mail or two-way via API) in comments.
3. Integration with external directories for workflow assignments.
4. Describe the content provided for threat descriptions (sources of content, competitive differentiation, etc.).
5. Describe the content provided for remediation advice (sources of content, competitive differentiation, etc.).

Report Capabilities

1. Predefined reports — how many? — and provide a general description of report types.
2. User-configurable reports (describe capability).
3. Describe predefined user activity monitoring and reports.
4. Describe support for privileged user monitoring and reports.
5. Indicate support for reporting with respect to specific regulations, and be specific about each regulation.
6. Indicate reporting with respect to specific control standards and security best practices.

Asset Classification

1. Describe product support for automatic asset grouping and classification by network segment, operating system, application, etc.
2. Describe product support for client-defined asset grouping and classification.
3. Describe product support for import of asset classification data.
4. Can the product maintain asset data and report by Media Access Control (MAC) address and host name?

Platform Support

1. Windows (specify agent, API, system log, etc.).
2. Red Hat Linux (specify agent, API, system log, etc.).
3. SUSE Linux (specify agent, API, system log, etc.).
4. Debian Linux (specify agent, API, system log, etc.).
5. Solaris (specify agent, API, system log, etc.).
6. AIX (specify agent, API, system log, etc.).
7. HP-UX (specify agent, API, system log, etc.).
8. Additional platforms defined by the user.

Network and Security Devices/Applications

1. Network devices defined by the user.
2. Firewalls defined by the user.
3. Intrusion detection system (IDS)/intrusion prevention system (IPS) devices defined by the user.
4. Network vulnerability assessment tools defined by user.
5. Endpoint protection tools defined by the user.
6. Additional security devices and applications defined by the user.

Database Activity Monitoring

1. Describe database-activity-monitoring capabilities, including platform and device connectors.
2. Describe agent or network monitor support for the collection of database activity data without a dependence on native DBMS audit logs.
3. Microsoft SQL Server support.
4. MySQL support
5. Oracle support.
6. DB2 support.
7. Additional DBMSs defined by the user.

Identity and Access Monitoring/Integration

1. Describe support for identity-oriented monitoring — real-time views and reporting.
2. Integration with IAM products, enterprise directories, or applications that enable identity-and-access-related policies to be established as a monitoring reference within the SIEM solution.
3. Describe specific support for IAM policy change monitoring (user/group permission changes, file/directory permission changes, etc.).
4. Describe Active Directory monitoring support.

5. IAM programs and enterprise directories defined by the user.

Application Integration

1. Describe monitoring and analysis support for application-layer-monitoring use cases.
2. Describe monitoring and analysis support for fraud detection use cases.
3. Packaged applications and in-house-developed applications defined by the user.
4. Fully document any proposed or available API.

3. Training

The successful respondent shall provide details and outline their capability to provide technical support training. Vendors will specifically address the following areas in their response:

- Training provided as part of purchase of hardware and/or software. This may include training vouchers other training credits identified by the course name and number these credits may be used towards and time limits for these credits if any.
- Types of training provided. Responses will differentiate between, on customer site, in class, on line or self study method of delivery.
- Variety of trainers. Responses shall provide information regarding training providers and nature of relation to the vendor. Examples- they are the same company, recommended training partner (authorized trainer)
- Capacity and location of training. Responses shall include number of trained staff and training locations within the MHEC states.

4. Maintenance

The successful contractor(s) shall provide an option for on-going support beyond the warranty and maintenance period as well as one (1), (2), (3), and (4) year options for product warranty and maintenance shall be included in the purchase price. Warranty and on-going support requirements are outlined below.

1. The warranty period shall begin upon successful installation and Eligible Participant acceptance of installation of the products acquired from respondent and covered by the purchase. Any warranty period of less than one year must be noted in your proposal.
2. Do you have 24/7 support? Where is it located? Is it staffed by your own employees, or is it a third-party facility?
3. Some institutions will require 24/7/365 coverage, and some will require less, please discuss the maintenance programs available. Do you offer on-site support if needed? What are the price differences between the programs?
4. Do you provide maintenance/support on customization implemented during the initial installation?
5. Does the maintenance program cover all future software upgrades? Explain.
6. Discuss your service call escalation policy — Level 1, Level 2 and so on.
7. Please describe the lifecycle of your equipment/service. How long after purchase can institutions renew maintenance?

I. Pricing

Technological advances are anticipated over the term of this contract. Vendors should include pricing in at least one of the following formats:

- Discount percentage from published retail price list
- Discount percentage from best published higher education price list
- Discount percentage from original purchase price (for support only)

Respondents may also propose alternate pricing arrangements in addition to those above. MHEC may choose to accept or reject such alternative arrangements.

In addition to purchase prices, the Respondent may offer a direct or indirect leasing program.

Some additional factors, which might modify pricing in the specific instances noted below, are:

- Eligible Participants who are willing to standardize their purchases to a small number of configurations should receive some consideration.
- Respondents offer a limited number preconfigured product selections discounted beyond their general product offerings.
- Eligible Participants that are willing to give an exclusive purchasing contract (of at least one year's duration) to a respondent should receive special consideration.
- Eligible Participants willing to guarantee purchase volume by year or quarter should be offered lower prices.
- Differential pricing based on market segment (e.g. higher education, K-12, local governments, state governments, faculty, staff or students) may be proposed.

Submission of innovative program ideas to increase vendor penetration of the market or satisfaction of the Eligible Participants as well as provide opportunity for stronger partnerships is encouraged.

Respondents are encouraged to provide a contract mechanism for their current eligible customers to roll into this agreement at anytime after the inception of the contract.

Successful Respondent agrees not to sell Awarded Products (or bundles) to Eligible Participants at a price higher than that awarded via the MHEC Master Price Agreement.

All pricing on future products offered under this proposal must, at a minimum, reflect the same percentage discounts or better as established with this contract award. Greater discounts are permissible and encouraged.

Any price reductions from suppliers from the time of proposal submission to time of purchase order must be passed on to the Eligible Participants.

Respondents must identify any and all associated costs, fees or charges for which the Eligible Participant may be billed. Costs not indicated in your proposal will not be paid.

1. Price/Fee Increases

MHEC reserves the right to accept or reject all or any part of successful supplier's subsequent request to increase pricing. At a minimum, any proposed price increase will become effective only upon thirty (30) days prior written notice and written acceptance by MHEC. In addition to the provision of an e-commerce web site for this contract, successful respondents will be expected to provide complete updated price lists to MHEC on a quarterly basis. All line item price increases or decreases and product additions or deletions must be identified.

Vendor must provide an identified capped annual increase rate for the life of the contract.

2. Certification of Independent Price Determination

By submitting a proposal, the vendor certifies, and in the case of a joint proposal, to its own firm, that in connection with this proposal:

1. The proposal has been arrived at independently, without consultation, communication or agreement with any competitor for the purpose of restricting competition, and;
2. Unless otherwise required by law, the offer cited in this proposal has not been and will not be knowingly disclosed by the vendor prior to opening directly or indirectly to any other vendor; and
3. No attempt has been made nor will be made by the vendor to induce another person or firm to submit or not to submit a proposal for the purpose of restricting competition.

J. Signatory Authority

Each person signing this proposal certifies that:

1. The signer is the person in the vendor's firm responsible for the decision to offer the proposal; or
2. The signer is not the person in the vendor's firm responsible within that firm for the decision to offer, but has been authorized in writing to act as agent to quote for the persons responsible for such decisions.

K. Conflict of Interest

In submitting a response to the RFP, the Provider certifies that no relationship exists between the Provider and the Midwestern Higher Education Compact or the members of its Security Products Committee that interferes with fair competition or is a conflict of interest, and that no relationship exists between the Provider, and other persons or firms that constitutes a conflict of interest that is adverse to the Midwestern Higher Education Compact.

L. RFP Development Process

1. Schedule of Events

The following schedule lists meetings and deadlines related to this Request For Proposal (RFP) on the development of a Master Price Agreement(s) for the MHEC Security Products Solution. Deadline dates are as indicated unless otherwise changed by the Committee. In the event that the Committee finds it necessary to change any of the dates

or activities listed in this calendar, it will do so by issuing a written statement or an amendment to the RFP to prospective Providers.

Event	Target Completion Date
1. Formal issuance of RFP	March 4, 2011
2. Last day for submitting inquiries about RFP by e-mail	5:00 pm CT March 11, 2011
3. Deadline to state Intent to participate in optional pre-proposal conference call	5:00 pm CT March 11, 2011
4. Pre-proposal conference call to review RFP	3:00 pm CT March 15, 2011
5. e-mail delivery to Prospective Providers of answers and amendment(s) to the RFP	March 18, 2011
6. Proposals due from Prospective Providers	April 15, 2011
7. Notification of Finalists	May 27, 2011
8. Individual meetings with Finalists (St. Louis) to review proposals submitted by each Prospective Provider Finalist (if required)	June 6-7, 2011
9. Deadline for submitting responses to Committee's questions and inquiries	June 15, 2011
10. Selection and announcement of Solution and Provider(s)	June 17, 2011
11. Execution of Agreement and Solution start date	August 1, 2011

M. Pre-proposal Conference and Requests for Clarification

Because of the straight-forward nature of this RFP, we will only use a one-stage process to answer questions. The question & answer stage will be conducted by e-mail and telephone conference, rather than through a bidders' meeting:

- Potential respondents must use e-mail to declare their intent to participate in the conference call by 5:00 pm CT March 11, 2011 in order that we might notify them of the call-in particulars.
- questions are to be submitted by e-mail no later than 5:00 pm CT March 11, 2011. If there are no questions, the subsequent conference call will be canceled.
- The conference call will take place 3:00 pm CT March 15, 2011 from 1:00 to 3:00 p.m. Central Time. During the call submitted questions will be addressed, as will any questions that come up during the call. Potential Respondents are strongly encouraged to participate in this call.
- Our answers will be provided to all potential respondents indicating participation by e-mail on March 18, 2011.

Information about the Compact, its member states, the Information Technologies Committee, the Security Products Committee and this RFP may be discussed. Requests for clarification, revisions to requirements or technical questions concerning the RFP may

be submitted to Mr. Grant Crawford at the MHEC office. Participation in the pre-proposal activities is voluntary. Prospective Providers should notify MHEC of their intention to participate in the pre-proposal activities by contacting Mr. Grant Crawford by e-mail at grantc@mhec.org

Those unable to participate in the pre-proposal conference call may submit requests for clarification, revisions to requirements, or technical questions concerning this RFP by e-mail. All written requests should arrive in our offices by 5:00 pm CT March 11, 2011. If a Prospective Provider discovers a significant ambiguity, error, conflict, discrepancy, omission, or other deficiency in the RFP, the Provider should *immediately* notify Mr. Grant Crawford of such error and request modification or clarification of the RFP document.

Only information supplied by MHEC in writing through Mr. Grant Crawford or this RFP or amended RFP should be used as a basis for the preparation of Provider responses.

N. Submission Deadlines and Format

The deadline for submission of proposals and related information is **5 p.m. Central Time on April 15, 2011. One (1) sealed bound original and nine (9) identical CD copies of the response should be forwarded to the following address prior to the deadline: Allowable formats are PDF and Microsoft Office. Spreadsheet data such as price lists may be submitted in MS Excel format. Proposals should be organized and presented in a manner that addresses all of the RFP provisions and requirements.**

Security Products Committee
c/o Mr. Grant Crawford
Midwestern Higher Education Compact
1300 South Second Street, Suite 130
Minneapolis, MN 55454-1015
Phone: (612) 626-8288
Fax: (612) 626-8290

O. Selection of Finalists and Best and Final Offers From Finalists

The Committee will select and notify the finalists on May 27, 2011. Only finalists will be invited to participate in the subsequent steps of the procurement. Prospective Provider Finalists may be asked to make a presentation to the Committee in St. Louis during the period June 6-7, 2011. Prospective Provider Finalists may be asked to submit revisions to their proposals for the purpose of obtaining best and final offers by June 15, 2011.

P. Provider Selection

All proposals received on or before the deadline date of submission will be forwarded to each Committee member. The Committee will conduct its evaluations of responses based upon its assessment of the quality and comprehensiveness of the Prospective Provider's responses to the criteria set forth in the RFP. During this initial evaluation time, the Committee may, at its option, initiate discussions with Prospective Providers who submit responsive or potentially responsive proposals for the purpose of clarifying aspects of the proposals, but proposals may be accepted and evaluated without such discussion. The Prospective Providers shall not initiate discussion. The Committee reserves the right to

waive or modify any informalities, irregularities or inconsistencies in the responses received. Following initial evaluations, Finalists will be selected. Each Prospective Provider Finalist will be invited to give a presentation on and discuss their response.

The Committee will evaluate each response based on the extent to which the proposal:

1. Meets the requirements of this RFP
2. Shows a willingness to explore solutions beyond a standard purchase agreement
3. Displays innovation

Award(s) may be granted to the highest scoring responsive and responsible proposer(s). Alternatively, the highest scoring proposer or proposers may be requested to submit best and final offers. Upon completion of the evaluation process, the Committee will recommend one or more Prospective Providers to the Commission, and the Commission will establish an agreement with the recommended Provider(s). Once an agreement(s) is successfully consummated, the Commission will so notify all providers who responded to the RFP. The Committee reserves the right to not recommend any Prospective Providers to the Commission, and the Commission reserves the right not to enter into an agreement with a recommended Provider at its own discretion.

After the Master Price Agreement(s) are executed, all proposals and documents pertaining to the proposals will be open to the public. If the Prospective Provider submits information in response to this RFP that it believes to be trade secret materials as defined by the laws of the MHEC member states, the Prospective Provider must:

- a. clearly mark all trade secret materials in its response at the time the response is submitted
- b. include a statement with its response justifying with specificity the trade secret designation for each item, and
- c. defend any action seeking release of the materials it believes to be a trade secret, and indemnify and hold harmless MHEC, its Commissioners, agents and employees, from any judgments awarded against MHEC in favor of the party requesting the materials, and any and all costs connected with the defense. This indemnification survives MHEC's award of a contract. In submitting a response to this RFP, the Prospective Provider agrees that this indemnification survives as long as the trade secret materials are in possession of MHEC.

In the event a request is made for information which the Prospective Provider has identified as trade secret, MHEC agrees to notify Prospective Provider of said request and provide its determination as to whether disclosure is legally required, in addition to anticipated disclosure dates, if any, and to allow the Prospective Provider an opportunity, in its discretion and at its sole expense, to seek a protective order or otherwise protect the confidentiality of the information.

Q. Contract Term

The MHEC Master Price Agreement shall be effective on the date that the parties to the Agreement sign the Agreement. It shall remain in effect for three (3) years from that date with options by mutual agreement (of the parties to the Agreement) to renew for up to four (4) additional one (1) year periods. Eligible Participants may procure hardware, software, or services from the Provider under the terms of the MHEC Master Price Agreement at any time during the duration of the Agreement.

R. Incurring Costs

MHEC is not liable for any cost incurred by Prospective Providers in replying to this RFP.

S. Method of Operation

The Committee, at the direction of the Commission and its compact authority, will negotiate the pricing structures, terms and conditions and related services provided under the Master Price Agreement(s). Any terms and conditions which may be the subject of negotiation, will be discussed only between MHEC and the selected Provider(s) and shall not be deemed an opportunity to amend the Provider's proposal. MHEC reserves the right to terminate negotiations and select the next response providing the best value for MHEC, prepare and release a new RFP, or take such other actions as MHEC deems appropriate if negotiations fail to result in a successful contract. Once a Master Price Agreement(s) is formally established, Eligible Participants will be responsible for procurement and payment of charges associated with the hardware, software, and related services provided to them. MHEC will not be liable for the failure of any Eligible Participant to make payment or for the breach of any term or condition under the Master Price Agreement.

The Commission will appoint a Committee composed of representatives of the MHEC Technologies Security Products Committee to oversee the solution and assure that it operates in an effective and efficient manner. The Commission will also assist in promoting the solution and assist Eligible Participants with problems as requested. The Committee will periodically review and evaluate the performance of the solution and submit its recommendations to the Commission. The Commission will provide program officer support to the solution, and will support information exchanges, conferences and related activities.

In advance of each contract anniversary representatives from each successful Respondent will meet separately with representatives from the Security Products Committee to discuss contract performance over the past year and amend the contract to improve its performance for the Respondent and Eligible Participants. These annual 'health checks' are crucial success factor.

The Commission, the members of the Technologies Committee and the members of the Security Products Committee make no guarantee that any Eligible Participant or number of Eligible Participants will participate in the MHEC Security Scanning & Audit Solution and/or make any purchase under the Master Price Agreement.

T. Analysis of Information

The Security Products Committee will analyze all responses to this RFP. The analysis will be based upon the criteria set forth in this RFP. The findings and recommendations of the Committee will be submitted to the MHEC President for approval.

U. Contacting MHEC

For further information about the Midwestern Higher Education Compact and its solutions you are referred to the Compact web site at: <http://www.mhec.org>

For Further information about the Compact's Technologies Committee or the Security Products Committee, contact:

Mr. Grant Crawford,
Chief Information Officer
Midwestern Higher Education Commission
1300 South Second Street, Suite 130
Minneapolis, MN 55454-1015
Phone: (612) 626-6383
Fax: (612) 626-8290
E-mail: grantc@mhec.org
Web Site: <http://www.mhectechnology.org>