Maine's Public Universities
UNIVERSITY OF MAINE SYSTEM

Administered by
UNIVERSITY OF MAINE SYSTEM
Office of Strategic Procurement

REQUEST FOR PROPOSALS

Security Monitoring Services – Information Technology
University of Maine System

RFP # 23-11

ISSUE DATE:
August 2, 2011

PROPOSALS MUST BE RECEIVED BY:
August 31, 2011

DELIVER PROPOSALS TO:

University of Maine System
Office of Strategic Procurement
Attn: Hal Wells
16 Central Street
Bangor, ME 04401

SECTION ONE

1.0 GENERAL INFORMATION:

1.1 Purpose: The University of Maine System wishes to solicit proposals from qualified Managed Security Service Providers (MSSPs) to provide monitoring and alerting services to the University of Maine System.

This Request for Proposals (RFP) states the instructions for submitting proposals, the procedure and criteria by which a vendor may be selected and the contractual terms by which the University intends to govern the relationship between it and the selected vendor.

1.2 Definition of Parties: The University of Maine System will hereinafter be referred to as the "University." Respondents to the RFP shall be referred to as "Bidder(s)" or "bidder(s)". The Bidder to whom the Contract is awarded shall be referred to as the "Contractor."

1.3 Scope: The required functions are as follows:

- Monitoring. 24 X 7 managed security and availability monitoring for behavior-based analysis to identify unusual traffic coming into and leaving the University's network as well as identify usual and unusual internal-to-internal traffic, aggregated and correlated from data collected from intrusion detection/prevention systems, firewalls, routers, and/or servers. Such monitoring will also gather information over time to address attacks that use a "low and slow" approach. Monitoring will be transmitted via secure means and accomplished in a way that limits bandwidth consumption.

- Analysis. 24 X 7 review of possible security events by qualified analysts in one or more Security Operations Centers (SOC) to analyze the nature of the events and take appropriate actions including classification of events based on specified Service Level Agreements (SLA's) and the nature of the event.

- Alert notification. 24 X 7 notifications to one or more University staff members based on calling trees which are dependent on the criticality and service affected. Notifications will include nature of the event and how to address such events.

- Recurring Review. Regular (at least quarterly) reporting on a summary of events to include recommendations on how to further prevent or mitigate such attacks and malicious activities.

- Optional Security Evaluation. Periodic external vulnerability scanning and periodic penetration testing will be identified as optional services.

- Warning notices. Provide information on zero day alerts.

1.4 Evaluation Criteria: Proposals will be evaluated on many criteria deemed to be in the University's best interests.

- The University intends to select a contractor who best demonstrates how they will meet the requirements of the University as set forth in this RFP.

- Total base price, upgrade service price and options prices will be considered when evaluating proposals. Price is not the only evaluation factor.

- Level of competence, reputation and viability. Bidders will be evaluated on their competency in IT security, level of certification of staff, and SOC certification. Bidders will also be evaluated on their company's financial stability, customer satisfaction/retention, company position with respect to its competition, its scale (overall device coverage), risk mitigation strategy and track record.

- Service Level Agreements. Bidders will provide copies of standard service level agreements (SLAs) which have been established and identify appropriate remediation in the event that there is a lapse in service levels.

- Scalability. Bidders shall provide evidence that their solution is scalable so that upgrading can occur during the life of the contract's option years. The proposal shall provide a base level of service with options for increased levels of service.

1.5 Communication with the University: It is the responsibility of the bidder to inquire about any requirement of this RFP that is not understood. Responses to inquiries, if they change or clarify the RFP in a substantial manner, will be forwarded by addenda to all parties that have received a copy of the RFP. Addenda will also be posted on our web site, www.maine.edu/strategic/upcoming_bids.php. The University will not be bound by oral responses to inquiries or written responses other than addenda.

Inquiries must be made to: Hal Wells
Office of Strategic Procurement
University of Maine System
16 Central Street
Bangor, Maine 04401
(207) 973-3302
hcwells@maine.edu

WRITTEN INQUIRIES SHALL BE SUBMITTED NO LATER THAN AUGUST 17, 2011
RESPONSES TO INQUIRIES WILL BE SENT NO LATER THAN AUGUST 24, 2011

1.6 Award of Proposal: Presentations may be requested of two or more bidders deemed by the University to be the best suited among those submitting proposals on the basis of the selection criteria. After presentations have been conducted, the University may select the bidder which, in its opinion, has made the proposal that is the most responsive and most responsible and may award the Contract to that bidder. The University reserves the right to waive minor irregularities. Scholarships, donations, or gifts to the University, will not be considered in the evaluation of proposals. The University reserves the right to reject any or all proposals, in whole or in part, and is not necessarily bound to accept the lowest cost proposal if that proposal is contrary to the best interests of the University. The University may cancel this Request for Proposals or reject any or all proposals in whole or in part. Should the University determine in its sole discretion that only one bidder is fully qualified, or that one bidder is clearly more qualified than any other under consideration, a contract may be awarded to that bidder without further action.

1.7 Award Protest: Bidders may appeal the award decision by submitting a written protest to the University of Maine System's Director of Strategic Procurement within five (5) business days of the date of the award notice, with a copy of the protest to the successful bidder. The protest must contain a statement of the basis for the challenge.

1.8 Confidentiality: The information contained in proposals submitted for the University's consideration will be held in confidence until all evaluations are concluded and an award has been made. At that time, the winning proposal will be available for public inspection. Pricing and other information that is an integral part of the offer cannot be considered confidential after an award has been made. The University will honor requests for confidentiality for information of a proprietary nature to the extent allowed by law. Clearly mark any information considered confidential.

1.9 Costs of Preparation: Bidder assumes all costs of preparation of the proposal and any presentations necessary to the proposal process.

1.10 Debarment: Submission of a signed proposal in response to this solicitation is certification that your firm (or any subcontractor) is not currently debarred, suspended, proposed for debarment, declared ineligible or voluntarily excluded from participation in this transaction by any State or Federal department or agency. Submission is also agreement that the University will be notified of any change in this status.

1.11 Proposal Understanding: By submitting a proposal, the bidder agrees and assures that the specifications are adequate, and the bidder accepts the terms and conditions herein. Any exceptions should be noted in your response.

1.12 Proposal Validity: Unless specified otherwise, all proposals shall be valid for ninety (90) days from the due date of the proposal.

1.13 Specification Protest Process and Remedies: If a bidder feels that the specifications are written in a way that limits competition, a specification protest may be sent to the Office of Strategic Procurement. Specification Protests will be responded to within five (5) business days of receipt. Determination of protest validity is at the sole discretion of the University. The due date of the proposal may be changed if necessary to allow consideration of the protest and issuance of any necessary addenda. Specification protests shall be presented to the University in writing as soon as identified, but no less than five (5) business days prior to the bid opening date and time. No protest against the award due to the specifications shall be considered after this deadline. Protests shall include the reason for the protest and any proposed changes to the specifications. Protests should be delivered to the Office of Strategic Procurement in sealed envelopes, clearly marked as follows:

SPECIFICATION PROTEST, RFP #23-11

1.14 Proposal Submission: A **SIGNED** original and three (3) copies of the proposal must be submitted to the Office of Strategic Procurement, University of Maine System, 16 Central Street, Bangor, Maine 04401, in a sealed envelope by **Wednesday, August 31, 2011**, to be date stamped by the Office of Strategic Procurement in order to be considered. Normal business hours are 8:00 a.m. to 5:00 p.m., Monday through Friday. Bidders may wish to check http://www.maine.edu/alerts/ to determine if University operations have been suspended.   Proposals received after the due date will be returned unopened. There will be no public opening of proposals (see Confidentiality clause). In the event of suspended University operations, proposals will be due the next business day. Vendors are strongly encouraged to submit proposals in advance of the due date to avoid the possibility of missing the due date because of unforeseen circumstances. Vendors assume the risk of the methods of dispatch chosen. The University assumes no responsibility for delays caused by any package or mail delivery service. Postmarking by the due date WILL NOT substitute for receipt of proposal. Additional time will not be granted to any single vendor, however additional time may be granted to all vendors when the University determines that circumstances require it. **FAXED OR E-MAIL PROPOSALS WILL NOT BE ACCEPTED**. The envelope must be **clearly** identified on the outside with the name of bidder, address of bidder, due date and “RFP #23-11”.

SECTION TWO

2.0 GENERAL TERMS AND CONDITIONS:

2.1 Contract Documents: If a separate contract is not written, the Contract entered into by the parties shall consist of the RFP, the signed proposal submitted by the Contractor, the specifications including all modifications thereof, and a purchase order or letter of agreement requiring signatures of the University and the Contractor, all of which shall be referred to collectively as the Contract Documents.

2.2 Contract Modification and Amendment: The parties may adjust the specific terms of this Contract (except for pricing) where circumstances beyond the control of either party require modification or amendment. Any modification or amendment proposed by the Contractor must be in writing to the Contract Administrator. Any agreed upon modification or amendment must be in writing and signed by both parties.

2.3 Contract Term: Unless other provisions are made, the initial term of this Contract shall begin as of the date of last signature (execution of the Contract). The University is seeking proposals for two (2) years of monitoring service with three (3) option years. The University will consider alternate proposals for a contract term of three (3) years with two (2) option years.

2.4 Contract Administration: The Chief Information Security Office for the University of Maine System, John Forker 207-973-3293 or his designee shall be the University's authorized representative in all matters pertaining to the administration of this Contract.

2.5 Employees: The Contractor shall employ only competent and satisfactory personnel and shall provide a sufficient number of employees to perform the required services efficiently and in a manner satisfactory to the University. If the Contract Administrator or designee, notifies the Contractor in writing that any person employed on this Contract is incompetent, disorderly, or otherwise unsatisfactory, such person shall not again be employed in the execution of this Contract without the prior written consent of the Contract Administrator.

2.6 Payments: Payment will be upon submittal of an invoice to the address shown on the purchase order by the Contractor on a Net 30 basis unless discount terms are offered. Invoices must include a purchase order number. The University is using several, preferred methods of payment: PCard (Visa); Bank of America’s ePayables and PayMode electronic payment systems. Please indicate your ability to accept payment via any or all of these methods.

2.7 Contract Data: The Contractor is required to provide the University with detailed data concerning the Contract at the completion of each contract year or at the request of the University at other times.

2.8 Contract Validity: In the event one or more clauses of the Contract are declared invalid, void, unenforceable or illegal, that shall not affect the validity of the remaining portions of the Contract.

2.9 Non-Waiver of Defaults: Any failure of the University to enforce or require the strict keeping and performance of any of the terms and conditions of this Contract shall not constitute a waiver of such terms, conditions, or rights.

2.10 Cancellation/Termination: If the Contractor defaults in its agreement to provide services to the University's satisfaction, or in any other way fails to provide service in accordance with the contract terms, the University shall promptly notify the Contractor of such default and if adequate correction is not made within ten (10) days, the University may take whatever action it deems necessary to provide alternate services and may, at its option, immediately cancel this Contract with written notice. Except for such cancellation for cause by the University, either the University or the Contractor may terminate this Contract by giving sixty (60) days advance written notice to the other party. Cancellation does not release the Contractor from its obligation to provide goods or services per the terms of the Contract during the notification period.

2.11 Clarification of Responsibilities: If the Contractor needs clarification of or deviation from the terms of the Contract, it is the Contractor's responsibility to obtain written clarification or approval from the Office of Strategic Procurement.

2.12 Litigation: This Contract and the rights and obligations of the parties hereunder shall be governed by and construed in accordance with the laws of the State of Maine without reference to its conflicts of laws principles. The Contractor agrees that any litigation, action or proceeding arising out of this Contract, shall be instituted in a state court located in the State of Maine.

2.13 Assignment: Neither party of the Contract shall assign the Contract without the prior written consent of the other, nor shall the Contractor assign any money due or to become due without the prior written consent of the University.

2.14 Equal Opportunity: In the execution of the Contract, the Contractor and all subcontractors agree, consistent with University policy, not to discriminate on the grounds of race, color, religion, sex, sexual orientation, transgender status or gender expression, national origin or citizenship status, age, disability or veteran’s status and to provide reasonable accommodations to qualified individuals with disabilities upon request. The University encourages the employment of individuals with disabilities.

2.15 Independent Contractor: Whether the Contractor is a corporation, partnership, other legal entity, or an individual, the Contractor is an independent contractor. If the Contractor is an individual, the Contractor's duties will be performed with the understanding that the Contractor is a self-employed person, has special expertise as to the services which the Contractor is to perform and is customarily engaged in the independent performance of the same or similar services for others. The manner in which the services are performed shall be controlled by the Contractor; however, the nature of the services and the results to be achieved shall be specified by the University. The Contractor is not to be deemed an employee or agent of the University and has no authority to make any binding commitments or obligations on behalf of the University except as expressly provided herein. The University has prepared specific guidelines to be used for contractual agreements with individuals (not corporations or partnerships) who are not considered employees of the University.

2.16 Sexual Harassment: The University is committed to providing a positive environment for all students and staff. Sexual harassment, whether intentional or not, undermines the quality of this educational and working climate. The University thus has a legal and ethical responsibility to ensure that all students and employees can learn and work in an environment free of sexual harassment. Consistent with the state and federal law, this right to freedom from sexual harassment was defined as University policy by the Board of Trustees.

Failure to comply with this policy could result in termination of this Contract without advanced notice.

Further information regarding this policy is available from Sally Dobres, Director of Equity and Diversity, (207) 973-3372.

2.17 Indemnification: The Contractor agrees to be responsible for, and to protect, save harmless, and indemnify the University and its employees from and against all loss, damage, cost and expense (including attorney's fees) suffered or sustained by the University or for which the University may be held or become liable by reason of injury (including death) to persons or property or other causes whatsoever, in connection with the operations of the Contractor or any subcontractor under this agreement.

2.18 Contractor's Liability Insurance: During the term of this agreement, the Contractor shall maintain the following insurance:

Insurance Type	Coverage Limit
1. Commercial General Liability (Written on an Occurrence-based form)	$1,000,000 per occurrence or more (Bodily Injury and Property Damage)
2. Vehicle Liability (Including Hired & Non-Owned)	$1,000,000 per occurrence or more (Bodily Injury and Property Damage)
3. Workers Compensation	Required for all personnel (In Compliance with Applicable State Law)

The University of Maine System shall be named as Additional Insured on the Commercial General Liability insurance.

Certificates of Insurance for all of the above insurance shall be filed with:

Office of Strategic Procurement
University of Maine System
16 Central Street
Bangor, Maine 04401

Certificates shall be filed prior to the date of performance under this Agreement. Said certificates, in addition to proof of coverage, shall contain the standard statement pertaining to written notification in the event of cancellation, with a thirty (30) day notification period.

As additional insured and certificate holder, the University should be included as follows:

University of Maine System
16 Central Street
Bangor, Maine 04401

2.19 Smoking Policy: The University must comply with the "Workplace Smoking Act of 1985" and M.R.S.A. title 22, § 1541 et seq "Smoking Prohibited in Public Places." In compliance with this law, the University has prohibited smoking in all University System buildings except in designated smoking areas. This rule must also apply to all contractors and workers in existing University System buildings. The Contractor shall be responsible for the implementation and enforcement of this requirement within existing buildings.

2.20 Gramm Leach Bliley (GLB) Act (Confidentiality of Information): The Contractor shall comply with all aspects of the GLB Act regarding safeguarding confidential information.

SECTION THREE

3.0 SPECIFICATIONS: The University requires security monitoring services for an assortment of devices as well as additional, optional services.

3.1 MSS Monitoring: The University’s configuration of devices is dynamic and will change over the life of the contract. The baseline devices to be monitored is **likely** to be comprised of eight (8) IDS/IPS devices which will exist as various locations. Data from vulnerability scans of 1,500 servers will be provided to be included in the analysis. The baseline configuration is expected to look as follows:

Location	Link Utilization	IDS/IPS
Fort Kent (UMFK)	1 x 200 Mbit	1
Presque Isle (UMPI)	1 x 100 Mbit	1
Farmington (UMF)	1 x 200 Mbit	1
Machias (UMM)	1 x 100 Mbit	1
Orono - Internet facing		1
UMaine	1 x 700 Mbit	
ITS Colo	1 x 300 Mbit	
ITS Servers	1 x 1 Gbit	
ITS Desktops	1 x 1 Gbit	
Bangor - Internet facing		1
ITS	1 x 200 Mbit	
UMA	1 x 200 Mbit	
Augusta - Internet facing		1
UMA	1 x 200 Mbit	
ITS	1 x 200 Mbit	
Portland - Internet facing		1
ITS Desktops	1 x 100 Mbit	
ITS Servers	1 x 100 Mbit	
		8 IDS/IPS
Total estimated baseline security devices		8

Monitoring may be extended to include up to eight (8) firewall devices (one at each campus and one facing the System Office network), up to ten (10) internal IDS/IPS, and up to fifty (50) servers. PCI-DSS activities may include up to eleven (11) routers, up to fifty (50) switches, up to four (4) additional IDS/IPS’s, up to seven (7) additional firewalls, and up to 117 log files (from thirteen (13) POS servers, fifty-one (51) POS desktops, fifty-three (53) terminals).

Therefore, pricing shall be provided for monitoring, analysis and alert notification for the following devices:

IDS/IPS (1 GB – 5GB)
IDS/IPS (<1GB)
Firewall (1 GB – 5GB)
Firewall (<1 GB) Internal IDS/IPS (1 GB – 5GB)
Internal IDS/IPS (<1GB)
Server
Router
Switch
Desktop

Quantity pricing shall be identified as applicable. Price variances based on specific equipment shall be identified if needed. Pricing for varied scaling options will be accepted.

3.2 Additional/Optional Services: Please provide cost estimates for the following:

A. Vulnerability Management Solution for 1,500 servers.
Assume two (2) scanners would need to be deployed to support scheduled and adhoc scanning by up to eight (8) security administrators. Internal and external scanning is desired.

B. Managed Service for:

- 8 IDS/IPS for network segments
- 8 Firewalls for network segments

SECTION FOUR

4.0 PROPOSAL CONTENT:

Bidders shall ensure that all information required herein is submitted with the proposal. All information provided should be verifiable by documentation requested by the University. Failure to provide all information, inaccuracy or misstatement may be sufficient cause for rejection of the proposal or rescission of an award. Bidders are encouraged to provide any additional information describing operational abilities. Responses to each requirement below should be in order and clearly marked with the section number to which they respond.

4.1 Business Profile:

4.1.1 Describe your company's breadth of services offered to meet evolving security needs, including:

- Different service or plan levels
- Threat based alerting based on device configuration or vulnerability data
- "In the wild" day 0 and active exploit reporting and alerting
- Alerting based on emerging threat trends globally as well as industry specific.

4.1.2 Provide a copy of your most recent independent reviews of your MSSP service in the form of a SAS 70 type II, ISO27001 or other applicable certification.

4.1.3 Describe how any of the top research firms (i.e. Gartner, IDC, Forrester) have ranked your company as a leader among available MSSPs? As applicable, provide reprints of article written by industry analysts supporting this claim.

4.1.4 Provide the number of monitored and managed security service customers currently, and projected by the end of the year. Include industry, size of installation and type of service.

4.1.5 Describe all tiers of any tiered solutions offered and the SLA and offerings of each tier.

4.1.6 Provide details on your research and development efforts for products, services and day one vulnerability detection.

4.1.7 Describe IDS/IPS lease programs that you support

4.1.8 Describe your company's device monitoring technology, process flow, and direction in developing new technologies in the Monitored and Managed Security Services.

4.1.9 Describe any forensic service offerings beyond regular monitoring, alerting, and advisement services.

- In house forensic services for data residing at SOC
- On site forensics services for security events at customer
- Onsite response SLAs

4.2 Financial Proposal

4.2.1 Please provide service fees for additions, deletions, and changes to monitored devices and services, including quantity pricing and additional/optional services (Section 3.1 and 3.2)

4.2.2 Describe your billing structure for devices, including virtual devices.

4.2.3 Describe your flexibility in providing different levels of monitoring services for different devices or device classes within the environment.

4.3 Functionality

4.3.1 Describe your approach to Security Monitoring.

4.3.2 Provide a list of the devices you have the ability to monitor in the following categories: network IDS/IPS, host IDS/IPS, Event Logs (Windows; Unix, with any differences involving flavor), Firewalls.

4.3.3 Describe the event correlation that can be performed between all devices listed above. Explain the ability for correlation from the external side of the firewall through the endpoint.

4.3.4 Describe the your “correlation window”, or the span of time over which events are compared against each other.

4.3.5 Describe how you incorporate security scanner output into the monitoring process. What scanner output do you support? What scanner’s output provides the most valuable input to your process?

4.3.6 Describe any ability to report and alert on abnormal behavior that is outside the realm of “signatures”.

4.3.7 Describe any ability to detect traffic patterns to known malicious sites.

4.3.8 Provide or describe any third party vendors leveraged to detect day one attacks and vulnerability signatures.

4.3.9 Provide the following details about your company’s Security Operation Centers (SOCs):

- Detailed hours of support coverage for your SOCs
- SOC redundancy
- Control Environment
- Geographic locations and Client coverage areas for failover
- Location of Client data, specifically any data that will be sent or stored out of the US.
- Location of the SOC analysts as well as any analysis that will be performed out of the US.

4.3.10 Provide the following details regarding staffing for monitored services:

- Number of engineers and analysts assigned to an account
- Number of staff onsite at each SOC 24x7x365
- Number of customer accounts handled by each account representative
- Are staff permanently assigned to a customer for duration of contract?
- Provide roles and responsibilities of staff that will be involved in providing security monitoring service.
- Detail staff levels of support and escalation procedures
- Qualifications, skill sets and certifications of analysts
- What training is offered to staff, and what training is mandatory?
- Frequency of background checks or screening performed.

4.3.11 Provide the following details regarding your security monitoring service:

- Describe the technical architecture including agents, failover, and backend.
- Describe your service level agreements for monitoring and notification. Include your method for measuring compliance.
- What reporting mechanisms and metrics do you provide, including frequency of reporting? Please provide samples. Can they be customer created?
- Do you support ad-hoc reporting requests by the customer?
- Describe you method(s) of data communications to/from customer security devices. Include format, protocol, and direction of communication.
- Describe how events between disparate security devices are correlated, and your process to correlate world-wide events, and events by geographic region.
- Describe your process for handling changes and growth for a customer’s security infrastructure.
- Describe the lifecycle of a security event from onset to closure.
- Describe your incident response support for security events.
- Describe your false positive handling process.
- Describe your chain of custody process.
- Provide details on any hardware or software that will be required to implement your monitored services.
- What educational tools and courses will be provided to our staff to enable us to use the service you are providing effectively?
- Describe your process to support a new customer device including time frames.
- Describe your ability to monitor virtual devices.
- Describe any hardware required to be on site at University for your solution to work.
- Provide details regarding the archiving and disposal of our data.
- Describe your ticket generation and tracking processes well as your support structure
- Describe any processes in place to profile our security devices, and keep information updated.
- What is your estimated initial deployment timeframe?
- How long do you provide enhanced support for tuning a new installation?

4.3.12 Provide the following information regarding the portal interface:

- Type of interface(s) offered
- Levels of Access
- Communication method
- Reporting capabilities
- Support of ad-hoc reporting

4.3.13 Describe the process for establishing and maintaining notification trees. Include the levels of granularity by event type, event severity, device, time of day, and the ability to support rotating schedules of “on duty” local staff.

4.3.14 Describe your ability and method of providing security intelligence.

4.4 Payment Method: Indicate your ability to accept electronic payments. (Section 2.6)

4.5 References: Submit, with your proposal, a list of three references. These references should be agencies your firm has done business with in the past year **on projects with a similar scope to this one**. Provide company names with contact person and telephone number.

SIGNATURE PAGE

COMPANY NAME: ____

By: ________________________________
(Signature)

____
(Print Name)

____
(Title)

____
(Phone)

____
(Cell Phone)

____
(E-mail Address)

____
(Date)