Administered by University of Maine System
Office of Strategic Procurement
Request for Proposal (RFP)

Payment Card Industry (PCI) Data Security Penetration Testing

RFP #36-15

Proposal Deadline Date/Time: January 28, 2015, 4:00 p.m.

Submit To:
University of Maine System
Office of Strategic Procurement
Robinson Hall
46 University Drive
Augusta, Maine 04330
Attn: Robin Cyr, IT Sourcing Manager

Proposal Contact Information:

Strategic Sourcing Manager: Robin Cyr, IT Sourcing Manager
Email: robin.cyr@maine.edu **Phone:** (207) 621-3098

Table of Contents

SECTION 1

1.0 General Information

1.1 Purpose

The University of Maine System is seeking proposals to provide PCI Data Security Standard Penetration Testing as defined in this Request for Proposals (RFP) document. This document provides instructions for submitting proposals, the procedure and criteria by which the Provider(s) will be selected, and the contractual terms which will govern the relationship between the University and the awarded Bidder(s).

The University of Maine System is seeking proposals for services of internal/external penetration testing which will meet the minimum requirements as set forth by the PCI DSS SAQ (sections 11.3 and 11.3.4).

Bidders should review Section 2 of this RFP to see the full Scope of Services/Products required.

Though this RFP is primarily for University of Maine System, all campuses in the University of Maine System must be afforded the use of this solution, with all the same terms and conditions applicable to the various University locations.

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 Eligibility to Submit Bids

1.3.1 Public entities, private for-profit companies, and non-profit companies and institutions are invited to submit bids in response to this Request for Proposal.

1.4 Evaluation Criteria

Scoring Weights: The score will be based on a 100 point scale and will measure the degree to which each proposal meets the following criteria.

Submission Requirements	Category	Points
Section 5 (5.1-5.2)	Organization Qualifications, Experience, and Financial Stability	15
Section 5 (5.3)	References	5
Section 5 (5.4)	Economic Impact Within State of Maine	5
Section 5 (5.5)	Cost Proposal	30
Section 9 (9.1)	Specifications of Work to be Performed – Technical	45
	Total Points	**100**

Section 5 (5.5 Only) – Cost Proposal

The total cost proposed for conducting all the functions specified in this RFP will be assigned a score according to a mathematical formula. The lowest bid will be awarded the total points. Proposals with higher bids values will be awarded proportionately fewer points calculated in comparison with the lowest bid.

The scoring formula is:

(Lowest submitted cost proposal / cost of proposal being scored) x **(30)** = pro-rated score

No Best and Final Offers: The University will not seek a best and final offer (BAFO) from any Bidder in this procurement process. All Bidders are expected to provide their best value pricing with the submission of their proposal.

1.5 Timeline of Key Events

Reference Section	Event Name	Event Due Date and Time
Section 1, 1.6	Deadline for Written Communication	**January 21, 2015**
Section 1, 1.6	Response to Written Communication	**January 23, 2015**
Section 1, 1.15	Deadline for Proposal Submission	**January 28, 2015**
	Bid Announcement **(subject to change)**	**January 30, 2015**
	Contract Negotiations **(subject to change)**	**February 1 – 13, 2015**
	Estimated Contract Start Date **(subject to change)**	**February 16, 2015**

1.6 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**

It is the responsibility of all bidders to check the web site before submitting a response to ensure that they have all pertinent documents. The University will not be bound by oral responses to inquiries or written responses other than addenda.

Inquiries must be made to:

University of Maine System
Office of Strategic Procurement
Robinson Hall
46 University Drive
Augusta, Maine 04330
ATTN: Robin Cyr, IT Sourcing Manager

Email: **robin.cyr@maine.edu**

Refer to table in **Section 1, 1.5 Timeline of Key Events** for deadline requirements.

1.7 Award

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(s) which, in its opinion, has made the proposal that is the most responsive and most responsible and may award the Contract to that/those bidder(s). While the University prefers a single solution that is scalable to meet the needs of both large and small institutions, it reserves the right to award contract(s) to one or multiple vendors, which may include awards to bidders for a geographical area, if such award is in the best interest of the University.

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.

1.8 Award Protest

Bidders may appeal the award decision by submitting a written protest to the University of Maine System's Chief Procurement Officer 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.

1.9 Confidentiality

The information contained in proposals submitted for the University's consideration will be held in confidence until all evaluations are concluded and a vendor selected (the successful bidder). At that time the University will issue bid award notice letters to all participating bidders and the successful bidder's proposal may be made available to participating bidders upon request. After the protest period has passed and the contract is fully executed, 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.

The University must adhere to the provisions of the Maine Freedom of Access Act (FOAA), 1 MRSA §401 et seq. As a condition of accepting a contract under this section, a contractor must accept that, to the extent required by the Maine FOAA, responses to this solicitation, and any ensuing contractual documents, are considered public records and therefore are subject to freedom of access requests.

1.10 Costs of Preparation

Bidder assumes all costs of preparation of the proposal and any presentations necessary to the proposal process.

1.11 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.

1.12 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.

1.13 Proposal Validity

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

1.14 Non-Responsive Proposals

The University will not consider non-responsive bids or proposals, i.e., those with material deficiencies, omissions, errors or inconsistencies.

1.15 Proposal Submission

A **SIGNED** original and one virus-free electronic copy (e.g., CD, thumb drive) must be submitted to the **University of Maine System, Office of Strategic Procurement, Robinson Hall 46 University Drive, Augusta, Maine 04330** in a sealed envelope by the end of business on **January 28, 2015** 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.

FAXED OR E-MAIL PROPOSALS WILL NOT BE ACCEPTED. The envelope must be **clearly** identified on the outside as follows:

Name of Bidder
Address of Bidder
January 28, 2015
RFP # 36-15

1.16 Authorization

Any contract or agreement for services that will, or may, result in the expenditure by the University of $50,000 or more must be approved in writing by the Office of Strategic Procurement, Chief Procurement Officer and it is not approved, valid or effective until such written approval is granted.

1.17 Multi-Institutional

The University of Maine System, Office of Strategic Procurement reserves the right to authorize other University Institutions to use the contract(s) resulting from this RFP, if it is deemed to be beneficial for the University to do so.

SECTION 2

2.0 Scope of Work

Penetration testing will include internal and external testing on IPs covering University of Maine System Institutions. Although future engagements may allow for remote work, Bidders should plan to travel to each Institution to perform internal testing.

Level I Penetration Testing Deliverables - Penetration testing for each Institution will require testing for the IPs identified. Penetration testing will meet the minimum requirements of **PCI DSS 3.0 (sections 11.3 and 11.3.4),** as well as, meeting the following University requirements:

1. Penetration testing from both inside and outside the network.
2. Testing to validate any segmentation and scope-reduction controls.
3. Verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from in-scope systems.
4. Specify remediation.
5. Network-layer penetration tests to include components that support network functions as well as operating systems that are within scope of each segmented PCI cardholder environment.
6. Application-layer penetration tests (where applicable) that include the vulnerabilities noted in the **PCI DSS 3.0 Requirements (Sections 6.5.1 - 6.5.10).**
    a. 6.5.1 - Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws.
    b. 6.5.2 - Buffer overflows
    c. 6.5.3 - Insecure cryptographic storage
    d. 6.5.4 - Insecure communications
    e. 6.5.5 - Improper error handling
7. Provide a Level I findings report with identified remediations.

Level II Penetration Testing Deliverables - Additionally there may be Institutions which require penetration testing for specific web applications. Such requirements will include testing of the vulnerabilities noted in the **PCI DSS 3.0 Requirements (Sections 6.5.7 - 6.5.10**).

1. 6.5.7 - Cross-site scripting (XSS)
2. 6.5.8 - Improper access control (such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access to functions).
3. 6.5.9 - Cross-site request forgery (CSRF)
4. 6.5.10 - Broken authentication and session management
    - Verify that broken authentication and session management are addressed via coding techniques that commonly include:
        - Flagging session tokens (for example cookies) as “secure”
        - Not exposing session IDs in the URL

- Incorporating appropriate time-outs and rotation of session IDs after a successful login.

5. Provide a Level II findings report with identified remediations.

Service Engagement Forms – Once the initial Contract for Services "Agreement" is fully executed and as required by the University of Maine System to support their needs, the parties will develop jointly specific Services Engagement forms. The required format of this document is detailed in **Contract for Services, Rider E**. The form will be governed by all the terms in the Agreement. The Services Engagement form will be fully executed by the parties. University of Maine System may execute more than one agreement for services to support their needs over the term of the Agreement.

Current planned Year 1 scheduled activities are detailed in the table directly below and will form the deliverables required for the first Service Engagement form. Bidders should note the testing type and completion date for the testing.

Table 1

#	Institution Name	Location	IP	Testing Type Deliverable	Completion Date
1	University of Maine	Orono, Maine	11	Level I & II	March 27, 2015
2	University of Maine at Farmington	Farmington. Maine	7	Level I	March 27, 2015
3	University of Southern Maine	Portland, Maine	7	Level I	March 27, 2015
4	University of Maine at Augusta	Augusta. Maine	5	Level I	March 27, 2015

Additional Scope: The University will have the option to purchase additional services under this Agreement.

The Bidder shall permit product and services not covered herein to be added by mutual agreement, without voiding the provisions of the Master Level Agreement. The Bidder, for additional consideration, shall furnish such additional products and services to the University.

SECTION 3

3.0 General Terms and Conditions

3.1 Contract Administration

The Office of the Chief Procurement Officer or its designee shall be the University's authorized representative in all matters pertaining to the administration of this Contract.

3.2 Contract Documents

The Contract entered into by the parties shall consist of the University of Maine System Contract for Services (attached to this document), the RFP, the selected Bidder's proposal, including all appendices or attachments, 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.

3.3 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.

3.4 Contract Term

The Contract term shall be for a period of **three (3) years** commencing upon the completion of implementation and acceptance by the University. With mutual written agreement of the parties this Contract may be extended for two additional one year periods. The University will consider other contract terms at its discretion if proposed and in the best interest of the University.

3.5 Contract Quantities

The quantities shown on the cost proposal form are approximate only. The contractor shall cover the actual needs of the University throughout the term of the contract regardless of whether they are more or less than the quantities shown.

3.6 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. The University reserves the right to audit the Contractor's records to verify the data.

3.7 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.

3.8 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.

3.9 Cancellation/Termination

If the Contractor defaults in its agreement to provide personnel or equipment to the University's satisfaction, places University students or employees at significant risk of harm, 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 seventy-two (72) hours 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. Cancellation does not release the Contractor from its obligation to provide goods or services per the terms of the Contract during the notification period.

3.10 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.

3.11 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 Contract Administrator.

3.12 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.

3.13 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.

3.14 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, including transgender status or gender expression, national origin or citizenship status, age, disability, genetic information, 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.

3.15 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.

3.16 Gramm Leach Bliley (GLB) Act (Confidentiality of Information)

The Contractor shall comply with all aspects of the GLB Act regarding safeguarding confidential information.

3.17 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: Bank of America's ePayables and PayMode electronic payment systems. Please indicate your ability to accept payment via any or all of these methods.

3.18 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.

3.19 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. Automobile 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 State Law)

The **University of Maine System** shall be named as Additional Insured on the Commercial General Liability insurance and as additional insured and certificate holder.

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.

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

University of Maine System
Risk Manager
16 Central Street
Bangor, Maine 04401

3.20 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.

3.21 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.

The University of Southern Maine is a tobacco-free campus. This policy applies to faculty, staff, students, contractors, vendors and visitors. The use of tobacco and all smoking products is not permitted on any university-owned property, which includes but is not limited to, buildings, university grounds, parking areas, campus walkways, recreational and sporting facilities, and university or personally-owned, rented or leased vehicles.

Tobacco use by definition includes the possession of any lighted tobacco products, or the use of any type of smokeless tobacco, including but not limited to chew, snuff, snus, electronic cigarettes, and all other nicotine delivery devices that are non-FDA approved as cessation products.

3.22 Pricing:

All prices quoted shall remain firm for the entire term of the agreement.

SECTION 4

4.0 Proposal Submission Requirements

This section contains instructions for Bidders to use in preparing their proposals. The Bidder's proposal must follow the outline used below, including the numbering and section and sub-section headings as they appear here. Failure to use the outline specified in this section or to respond to all questions and instructions throughout this document may result in the proposal being disqualified as non-responsive or receiving a reduced score. The University and its evaluation team for this RFP have sole discretion to determine whether a variance from the RFP specifications should result in either disqualification or reduction in scoring of a proposal. Re-phrasing of the content provided in this RFP will, at best, be considered minimally responsive. The University seeks detailed yet succinct responses that demonstrate the Bidder's experience and ability to perform the requirements specified throughout this document.

Responses to each requirement below should be in order and clearly marked with the section number to which they respond.

4.1 Format

4.1.1 Proposals are to be prepared on standard 8-1/2" x 11" paper. Foldouts containing charts, spreadsheets, and oversize exhibits are permissible. The pages should be placed in a binder with tabs separating the sections of the bid. Manuals and other reference documentation may be bound separately.

4.1.2 All pages should be numbered consecutively beginning with number 1 on the first page of the narrative (this does not include the cover page or table of contents pages) through to the end, including all forms and attachments. For clarity, the Bidder's name should appear on every page, including Attachments. Each Attachment must reference the section or subsection number to which it corresponds.

4.1.3 Bidders are asked to be brief and to respond to each question and instruction listed in the "Submission Requirements" section of this RFP. Number each response in the proposal to correspond to the relevant question or instruction this document.

4.1.4 The Bidder may not provide additional attachments beyond those specified in the RFP for the purpose of extending their response. Any material exceeding the bid limit will not be considered in rating the bid and will not be returned. Bidders shall not include brochures or other promotional material with their bid. Additional materials will not be considered part of the bid and will not be evaluated.

4.1.5 Include any forms provided in the application package or reproduce those forms as closely as possible. All information should be presented in the same order and format as described in this document.

4.1.6 Bidders must complete and submit the bid cover page provided in **Appendix A** of this RFP and provide it with the Bidder's bid. The cover page must be the first page of the bid. It is important that the cover page show the specific information requested, including Bidder address(es) and other details listed. The bid cover page shall be dated and signed by a person authorized to enter into contracts on behalf of the Bidder.

4.1.7 It is the responsibility of the Bidder to provide all information requested in the RFP package at the time of submission. Failure to provide information requested in this RFP may, at the discretion of the University's evaluation review team, result in a lower rating for the incomplete sections and may result in the proposal being disqualified for consideration.

4.1.8 **Content Format**

The proposal shall be submitted under the same cover at the same time, in the five (5) distinct sections noted below:

Section I Organization Qualifications and Experience

1. Appendix A – University of Maine System Bid Cover Page and table of contents.
2. Provide responses for each requirement in Section 5:
    a. 5.1 Organizational Qualifications and Experience
    b. 5.2 Financial Stability
    c. 5.3 References
    d. 5.4 Economic Impact within the State of Maine
3. Attach a certificate of insurance on a standard Acord form (or the equivalent) evidencing the Bidder's general liability, professional liability and any other relevant liability insurance policies that might be associated with this contract. See 2.16 Contractor's Liability Insurance.
4. Attach a Form W-9 or Form W-8 if you are a foreign person, or complete document provided in Rider B-2 of the University of Maine, Contract for Services

Section II Cost Proposal

1. Provide responses for each requirement in Section 5:
    a. 5.5 Cost Proposal – Exhibit 1 referenced in Appendix B.

Section III Proposed Services

1. Provide responses for each requirement in Section 9:
    a. 9.0 Technical Requirements

Section IV Contract for Services

1. Provide copy of the University of Maine, Contract for Services with the required responses as outlined in Section 6.

Section V. Attachments

1. Any remaining attachments required as part of the response.

SECTION 5

5.0 Organizational Qualifications, Experience, Financial Stability, References & Costs

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.

5.1 Organizational Qualifications and Experience

5.1.1 Provide a statement describing your company to include name, number of employees, locations, number of years in business, number of years offering/supporting the proposed solution, and any and all acquisitions or mergers in the last five years. Is the company publicly or privately held

5.1.2 Please provide information about contract cancellations or non-renewals your company has experienced over the last three years.

5.1.3 Provide a statement that explains why your company would be most qualified to provide products and services to the University of Maine System. What differentiates you from your competitors? In the response the Bidder must demonstrate that they are a recognized leader in the services and/or products covered in this RFP.

5.1.4 The Bidder shall provide a description of its employee workforce descriptions shall include a summary of experience to include technical qualifications and Professional Credentials education.

5.2 Financial Stability

No financial statements are required to be submitted with your proposals, however, prior to an award the University may request financial statements from your company, credit reports and letters from your bank and suppliers.

5.3 References

Provide at least three (3) current professional references who may be contacted for verification of the bidder's professional qualifications to meet the requirements set forth herein. We will request that the references include one long-standing customer (minimum of 3 year engagement) and one new customer (one who has been engaged with vendor for less than one year). We strongly prefer clients from higher education institutions similar in size and requirements to the University of Maine System, including those with multi-campus integrated solutions.

5.4 Economic Impact within the State of Maine

In addition to all other information requested within this RFP, each Bidder must dedicate a section of its proposal to describing the Bidder's economic impact upon and within the State of Maine.

For the purposes of this RFP, the term "economic impact" shall be defined as any activity that is directly performed by or related to the Bidder and has a direct and positive impact on the Maine economy and public revenues within the State of Maine. Examples may include, but are not limited to, employment of Maine residents, subcontracting/partnering with Maine businesses, payment of State and Local taxes (such as corporate, sales, or property taxes), and the payment of State licensing fees for the Bidder's business operations.

To complete the "economic impact" section of the Bidder's proposal, the Bidder shall include no more than one page of typed text, describing the Bidder's current, recent, or projected economic impact with the State of Maine, as defined above. The Bidder may include all details and information that it finds to be most relevant for this section.

5.5 Cost Proposal

5.5.1 General Instructions:

5.5.1.1 The Bidder must submit a cost proposal that covers the entire period of the contract, including any optional renewal periods. Please use the expected contract start date of **February 16, 2015** and an end date of **February 15, 2018** with option for **two (2) one (1) year renewals** in preparing this section.

5.5.1.2 The cost proposal shall include the costs necessary for the Bidder to fully comply with the contract terms and conditions and RFP requirements.

5.5.1.3 Failure to provide the requested information and to follow the required cost proposal format provided in Appendix B may result in the exclusion of the proposal from consideration, at the discretion of the University.

5.5.1.4 No costs related to the preparation of the proposal for this RFP or to the negotiation of the contract with the University may be included in the proposal. Only costs to be incurred after the contract effective date that are specifically related to the implementation or operation of contracted services may be included.

5.5.2 Cost Proposal Form Instructions – Appendix B

5.5.2.1 The Bidder **MUST** fill out **Exhibit 1** referenced in **Appendix B**, following the instructions detailed in Appendix B. For a copy of the excel version of Exhibit 1, email the contact provided in **Section 1.6.**

SECTION 6

6.0 Contract for Services Requirements

6.1 The winning Bidder must enter into a formal University of Maine System Contract for Services, which is attached to this proposal, **University of Maine System, Contract for Services**. The award will be **three (3) years** with **two (2) one (1) year** renewal options.

As part of the Bid response each Bidder is required to provide as part of their bid submission the following:

6.1.1 Provide either a **red-line version** to reflect language adjustments to the University of Maine System, Contract for Services, "Agreement".

For a copy of the word version of the Agreement email the contact provided in **Section 1.6**.

OR

Sign the Agreement signifying acceptance of the terms and conditions, Riders, the RFP and the Bidder's proposal, including all appendices or attachments, are incorporated in the final Agreement.

6.1.2 Provide University of Maine System, Contract for Services, language for **Rider D Implementation Plan and Timeline.**

The Implementation Plan and Timeline must reflect a high-level milestone plan with estimated duration for the implementation.

6.1.3 Provide University of Maine System, Contract for Services language for **Rider G Contractor's Service Level Agreement to Support the University**.

Service Level Agreement (SLA) will include at a minimum a description of the agreement between the Contractor and the University through the documentation of IT Services, including but not limited to, Service Level Targets and specifies the responsibilities of the IT Service Provider and the University. The general structure of the agreement should include:

Service Description, Service Hours, Service Availability, Reliability, Customer Support, Service Performance, Functionality, Change Management Procedure, Service Reviews, Glossary of Terms, Amendment Sheet (as applicable).

SECTION 7

7.0 Business Functional Requirements (Matrix Section)

Section 7 is intentionally left blank.

SECTION 8

8.0 Business Functional Requirements (Narrative Section)

Section 8 is intentionally left blank.

SECTION 9

9.0 Technical Requirements

All responses to the requirements should reflect delivered, or out-of-the-box, functionality. Bidders **MUST** indicate if system modification, additional products or vendors, costs or if any other accommodation would be necessary to meet a requirement.

Responses to each requirements below should be in order and clearly marked with the section number to which they respond.

9.1 Technical Requirements – General

9.1.1 Describe your process for performing PCI DSS Penetration Testing as to meet the minimum requirements set forth by PCI DSS 3.0.

9.1.2 Describe your penetration testing framework – which industry-accepted penetration testing approach(es) are utilized.

9.1.3 Describe how your penetration tests differ from other type of security testing – such as vulnerability assessments.

9.1.4 Describe how you will ensure the availability of University systems and services while the penetration test is taking place.

9.1.5 Describe your approach to informing the University if an immediate threat is discovered during the penetration testing.

9.1.6 Describe how you will protect University data during and after testing.

9.1.7 Please read and confirm that you agree with the attached document, Standards for Safeguarding Information.

9.1.8 Describe your availability to being able to complete the penetration tests within the timetable set in section **2.0 Scope of Work**. Additionally describe your expected lead time for future engagements.

9.1.9 Final Deliverable Report: Please provide an example of what a final deliverable report will look like and how soon will it be available after external/internal penetration testing is complete.

9.1.10 Provide confirmation that you can meet the complete date for the deliverables noted in **Section 2 Scope of Work, Table 1**.

SECTION 10

10.0 List of Appendices and Related Documents

This section lists documents which are included in the RFP.

10.1 Appendix A – University of Maine System Proposal Cover Page

10.2 Appendix B – Cost Proposal Form

10.3 Exhibit 1 – Pricing

10.4 University of Maine System, Contract for Services

Appendix A – University of Maine System Quote Vendor Page

RFP # 36-15
Payment Card Industry (PCI) Data Security Penetration Testing

Organization Name:	
Chief Executive – Name/Title:	
Telephone:	
Fax:	
Email:	
Headquarters Street Address:	
Headquarters City/State/Zip:	
Lead Point of Contact for Quote – Name/Title:	
Telephone:	
Fax:	
Email:	
Street Address:	
City/State/Zip:	

- This quote and the pricing structure contained herein will remain firm for a period of 90 days from the date and time of the quote deadline date.
- No personnel currently employed by the University or any other University agency participated, either directly or indirectly, in any activities relating to the preparation of the Bidder's quote.
- No attempt has been made or will be made by the Bidder to induce any other person or firm to submit or not to submit a quote.
- The undersigned is authorized to enter into contractual obligations on behalf of the above-named organization.

To the best of my knowledge all information provided in the enclosed quote, both programmatic and financial, is complete and accurate at the time of submission.

Authorized Signature Date Name and Title (Typed)

Appendix B - Cost Proposal Form

University of Maine System
COST PROPOSAL FORM

RFP # 36-15
Payment Card Industry (PCI) Data Security Penetration Testing

Bidder's Organization Name:

_____

GENERAL INSTRUCTIONS:

Identify all costs by year, to be charged for performing the services necessary to accomplish the objectives of the contract.

Note regarding total cost of ownership: This "cost" will encompass the entire solution pricing along with all services. This includes any software, licenses, equipment, professional services, customization costs necessary to complete the work specified in the Scope of Work. All items identified in the proposal (including third party items required) will be considered free add-ons to the proposed solution at the prices included in this RFP response unless expressly stated otherwise.

IMPORTANT – Please do NOT change any formatting on the response sheet in any manner (such as merged cells). You can add rows required to insert additional information. If a particular cost table is not required as part of your proposal simply leave it blank.

INSTRUCTIONS FOR - Exhibit 1 (Table 1) –Penetration Testing Pricing for Section 2.0 Scope of Work Table 1 Identified Testing Activities

The Bidder is to submit the cost for the testing activities identified in **Section 2.0 Scope of Work Table 1** identified testing activities.

The hourly rate shall be inclusive of staff costs, administrative costs, and any other expenses necessary to accomplish the tasks and to produce the deliverables under the contract. If the Bidder costing model includes other factors in calculation of cost, such as number of IPs, than the Bidder may add the appropriate column to the table.

Travel costs for **Section 2.0 Scope of Work Table 1** identified testing activities will be provided in **Exhibit 1 Table 3**.

Req. Hours is the required hours to complete the testing identified. Details on requirements for Level I and Level II testing can be found in **Section 2 Scope of Work.**

Hourly Rate (for each year) is the hourly dollar amount that will be invoiced as a result of completing the testing identified in the Penetration Testing column. You shall warranty your work for a period of ninety (90) days from date of University's acceptance.

Exhibit 1 (Table 1) –Bidders will use this attachment, specifically Table 1 to record all costs associated with this section. For a copy of the excel version of Exhibit 1, email the contact provided in **Section 1.6.**

INSTRUCTIONS FOR - Exhibit 1 (Table 2) – Level I and Level II Penetration Testing Pricing

The Bidder is to submit number of hours and hourly rate to complete **Level I and Level II Penetration Testing**, as detailed in **Section 2 Scope of Work** of this RFP. The hourly rate shall be inclusive of staff costs, administrative costs, and any other expenses necessary to accomplish the tasks and to produce the deliverables under the contract. If the Bidder costing model includes other factors in calculation of cost, such as number of IPs, than the Bidder may add the appropriate column to the table.

Req. Hours is the required hours to complete the testing identified. Details on requirements for Level I and Level II testing can be found in **Section 2 Scope of Work.**

Hourly Rate (for each year) is the hourly dollar amount that will be invoiced as a result of completing the testing identified in the Penetration Testing column. You shall warranty your work for a period of ninety (90) days from date of University's acceptance.

Optional Renewal (for each year) is the hourly dollar amount that will be invoiced as a result of completing the testing identified in the Penetration Testing column. You shall warranty your work for a period of ninety (90) days from date of University's acceptance.

Exhibit 1 (Table 1) –Bidders will use this attachment, specifically Table 1 to record all costs associated with this section. For a copy of the excel version of Exhibit 1, email the contact provided in **Section 1.6.**

INSTRUCTIONS FOR - Exhibit 1 (Table 3) – Travel Expenses

The Bidder is to submit all related travel expenses associated with each location identified in the table.

Year 1 Cost is the cost for travel to the Institution/location identified for Year 1.

Year 2 Cost is the cost for travel to the Institution/location identified for Year 2.

Year 3 Cost is the cost for travel to the Institution/location identified for Year 3.

Optional Renewal (for each year) is the cost for travel to the Institution/location identified.

Exhibit 1 (Table 2) –Bidders will use this attachment, specifically Table 2 to record all costs associated with this section. For a copy of the excel version of Exhibit 1, email the contact provided in **Section 1.6.**

Section 2.0 Scope of Work Table 1
Identified Testing Activities

#	Institution Name	Location	IP	Testing Type Deliverable	Req Hours	Total Cost
1	University of Maine	Orono, Maine	11	Level I & II		
2	University of Maine at Farmington	Farmington. Maine	7	Level I		
3	University of Southern Maine	Portland, Maine	7	Level I		
4	University of Maine at Augusta	Augusta. Maine	5	Level I		
5						
6						
7						
8						
9						
10						
	Include additional explanation of costs and list assumptions that could influence the cost of change request pricing.					
	List explanations and assumptions here;					
	-					
	-					
	-					
	-					
	-					

TABLE 2

Level I and Level II Penetration Testing Pricing

#	Pentration Testing	Req Hours	Hourly Rate (Year 1)	Hourly Rate (Year 2)	Hourly Rate (Year 3)	Optional Renewal (Year 1)	Optional Renewal (Year 2)
1	Level I Penetration Testing Deliverables						
2	Level II Penetration Testing Deliverables						
3							
4							
5							
6							
7							
8							
9							
10							
	Include additional explanation of costs and list assumptions that could influence the cost of change request pricing.						
	List explanations and assumptions here;						
	-						
	-						
	-						
	-						
	-						

TABLE 3

Travel Expenses

#	Travel Cost	Year 1 Cost	Year 2 Cost	Year 3 Cost	Optional Renewal (Year 1)	Optional Renewal (Year 2)
1	University of Maine, Orono, Maine					
2	University of Southern Maine, Portland, Maine					
3	University of Maine at Augusta, Augusta, Maine					
4	University of Maine at Augusta, Bangor, Maine					
5	University of Maine at Farmington, Farmington, Maine					
6	University of Maine at Machias, Machias Maine					
7	University of Maine at Presque Isle, Presque Isle, Maine					
8	University of Maine at Fort Kent, Fort Kent, Maine					
9						
10						
	List explanations and assumptions here					
	-					
	-					
	-					
	-					
	-					

UNIVERSITY OF MAINE SYSTEM
CONTRACT FOR SERVICES

This Master Level Agreement entered into this _____ day of _____**,** _____**,** by and between the **University of Maine System**, hereinafter referred to as the **"University",** and _____, hereinafter referred to as **"Contractor".**

WITNESSETH, that for and in consideration of the payments and agreements hereinafter mentioned, to be made and performed by the University, the Contractor hereby agrees with the University to provide the products and services described in this agreement, and the following Riders, hereby incorporated into this Agreement and made part of it by reference:

Rider A - Specifications of Work to be Performed
Rider A-1 – Pricing
Rider B-1 – Insurance Requirements
Rider B-2 – Substitute Form W-9 - Taxpayer Identification Number Request & Certification
Rider C – University of Maine System Standards for Safeguarding Information
Rider D – Implementation Plan and Timeline
Rider E – Services Engagement Form
Rider F – Contractor's Service Level Agreement to Support the University

Contract Amendments as required
Request for Proposal #36-15 Dated January 16, 2015 Titled Payment Card Industry (PCI) Data Security Penetration Testing
Contractor's Bid in Response to Request for Proposal #36-15 Proposal Submission Date January 28, 2015 **Titled** Payment Card Industry (PCI) Data Security Penetration Testing

WHEREAS, the University desires to enter into a contract for professional services, and the Contractor represents itself as competent and qualified to accomplish the specific requirements of this Contract to the satisfaction of the University;

NOW THEREFORE, in consideration of the mutual promises contained herein, the parties hereby agree as follows:

This Agreement, along with any documents identified, which are incorporated by reference, constitutes the entire Agreement between the parties, and there are no other or further written or oral understandings or agreements with respect thereto.

1. **Specifications of Work:** The Contractor agrees to perform the Specifications of Work as described in **Attachment A**, hereby incorporated by reference.
   Rider A provides a suite of services offered by the Contractor to the University. As required by the University institutions, the parties will develop jointly specific Services Engagement documents. The required format of this document is detailed in **Rider E**. The document will be governed by all the terms in this agreement; except that the engagement administrator for purposes of managing the service deliverables may be different than this Agreement Administrator and the term may be different than the term of the agreement but may not extend beyond this Agreement termination date. The Services Engagement document will be fully executed by the parties. Institutions may execute more than one agreement for services to support their needs over the term of this Agreement

2. **Term:** This Contract shall commence on **February 16, 2015** and shall terminate on **February 15, 2018**, unless terminated earlier as provided in this Contract with option **two (2) one (1) year renewals** upon the parities' mutual agreement.

3. **Payment:**

   A. Payment shall be made upon submittal of an electronic invoice to the University by the Contractor on a net 30 basis unless discount terms are offered. In the event there is a discrepancy with the invoice, payment terms shall be effective starting on the date the discrepancy is resolved, for only that portion of the invoice that is disputed. Invoices must include a purchase order number.

   B. **"Reimbursement for travel"** The University may purchase additional in-person training days which will not exceed the prices noted in Rider A-1, Pricing. Contractor will supply copies of travel receipts with the invoice for reimbursement.

   C. "**Additional Services**" As required by the University institutions, the parties will develop jointly specific Services Engagement documents. The required format of this document is detailed in **Rider E**.

   D. **"Multi-Institution Capabilities"** University will have the option to include products and services under this Agreement to additional University institutions, this includes any additional University institutions formed during the term of this agreement, all facilities utilized by an institution including those managed and/or owned by a third party, and additional entities, such as, the University College a division of University of Maine at Augusta.

4. **Termination:** The **Services Engagement Form (Rider E)** may be terminated by the University in whole, or in part, whenever for any reason the University shall determine that such termination is in the best interest of the University. Any such termination shall be effected by delivery to the Contractor of a Notice of Termination specifying the extent to which performance of the Agreement is terminated and the date on which such termination becomes effective. The University shall pay all allowable costs incurred up to the effective date of termination. However, the Contractor shall not be reimbursed for any costs incurred after the effective date of termination.

5. **Obligations Upon Termination:** Any materials produced in performance of this agreement are the property of the University and shall be turned over to the University upon request. The University shall pay the Contractor for all services performed to the effective date of termination subject to offset of sums owed by the Contractor to the University.

6. **Non-Appropriation:** Notwithstanding any other provision of this Agreement, if the University is not appropriated sufficient funds to pay for the work to be performed under this Agreement or if funds are de-appropriated, then the University is not obligated to make payment under this Agreement.

7. **Conflict of Interest:** No officer or employee of the University shall participate in any decision relating to this contract which affects his or her personal interest in any entity in which he or she directly or indirectly has interest. No employee of the University shall have any interest, direct or indirect, in this contract or proceeds thereof.

8. **Modification:** This Contract may be modified or amended only in a writing signed by both parties.

9. **Assignment:** This Contract, or any part thereof, may not be assigned, transferred or subcontracted by the Contractor without the prior written consent of the University.

10. **Applicable Law:** This Contract shall be governed and interpreted according to the laws of the State of Maine.

11. **Administration: John Forker** shall be the University's authorized representative in all matters pertaining to the administration of the terms and conditions of this Contract and to whom all notices must be sent.

12. **Non-Discrimination:** In the execution of the contract, the Contractor shall not discriminate on the basis of race, color, religion, sex, sexual orientation, transgender status or gender expression, national origin or citizenship status, age, disability, genetic information, or veteran status and shall provide reasonable accommodations to qualified individuals with disabilities upon request. The university encourages the employment of qualified individuals with disabilities.

13. **Indemnification:** The Contractor shall comply with all applicable federal, state and local laws, rules, regulations, ordinances and orders relating to the services provided under this Contract. Contractor shall indemnify, defend and hold the University, its Trustees, officers, employees, and agents, harmless from and against any and all loss, liability, claims, damages, actions, lawsuits, judgments and costs, including reasonable attorney's fees, that the University may become liable to pay or defend arising from or attributable to any acts or omissions of the Contractor, its agents, employees or subcontractors, in performing its obligations under this Contract, including, without limitation, for violation of proprietary rights, copyrights, or rights of privacy, arising out of a publication, translation, reproduction, delivery, performance, use or disposition of any data furnished under the Contract or based on any libelous or other unlawful matter contained in such data.

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

15. **Independent Contractor:** Contractor is an independent contractor of the University, not a partner, agent or joint venture of the University and neither Party shall hold itself out contrary to these terms by advertising or otherwise, nor shall either party be bound by any representation, act or omission whatsoever of the other. For U.S. entities, Contractor, its employees and subcontractors if any, is/are independent contractors for whom no Federal or State Income Tax will be deducted by the University, and for whom no retirement benefits, social security benefits, group health or life insurance, vacation and sick leave, Worker's Compensation and similar benefits available to University's employees will accrue. The parties further understand that annual information returns as required by the Internal Revenue Code and Maine Income Tax Law will be filed by the University with copies sent to Contractor. Contractor will be responsible for compliance with all applicable laws, rules and regulations involving but not limited to, employment, labor, Workers Compensation, hours of work, working conditions, payment of wages, and payment of taxes, such as unemployment, social security and other payroll taxes, including other applicable contributions from such persons when required by law.

16. **Intellectual Property:** Any information and/or materials, finished or unfinished, produced in performance of this Contract, and all of the rights pertaining thereto, are the property of the University and shall be turned over to the University upon request.

17. **Entire Contract:** This Contract sets forth the entire agreement between the parties on the subject matter hereof and replaces and supersedes all prior agreements on the subject, whether oral or written, express or implied.

18. **Licensing:** Contractor shall secure in its name and at its expense all federal, state, and local licenses and permits required for operation under this Contract. Contractor shall provide proof of such licensure or permit to the University prior to commencing work under this Contract.

19. **Record Keeping, Audit and Inspection of Records:** The Contractor shall maintain books, records and other compilations of data pertaining to the requirements of the Contract to the extent and in such detail as shall properly substantiate claims for payment under the Contract. All such records shall be kept for a period of seven years or for such longer period as specified herein. All retention periods start on the first day after the final payment of the Contract. If any litigation, claim, negotiation, audit or other action involving the records is commenced prior to the expiration of the applicable retention period, all records shall be retained until completion of the action and resolution of all issues resulting therefrom, or until the end of the applicable retention period, whichever is later. The University, the grantor agency (if any), or any of their authorized representatives shall have the right at reasonable times and upon reasonable notice, to examine and copy the books, records and other compilations of data of the Contractor pertaining to this Contract. Such access shall include on-site audits.

20. **Publicity, Publication, Reproduction and use of Contract's Products or Materials:** Unless otherwise provided by law or the University, title and possession of all data, reports, programs, software, equipment, furnishings and any other documentation or product paid for with University funds shall vest with the University. The Contractor shall at all times obtain the prior written approval of the University before it, any of its officers, agents, employees or subcontractors, either during or after termination of the Contract, makes any statement bearing on the work performed or data collected under this Contract to the press or issues any material for publication through any medium of communication. If the Contractor or any of its subcontractors publishes a work dealing with any aspect of performance under the Contract, or of the results and accomplishments attained in such performance, the University shall have a royalty free, non-exclusive and irrevocable license to reproduce, publish or otherwise use and to authorize others to use the publication.

21. **Confidentiality:** The contractor shall comply with all laws and regulations relating to confidentiality and privacy including but not limited to any rules or regulations of the University.

22. **Force Majeure:** Neither party shall be liable to the other or be deemed to be in breach of this Contract for any failure or delay in rendering performance arising out of causes beyond its reasonable control and without its fault or negligence. Such causes may include, but are not limited to, acts of God or of a public enemy, fires, flood, epidemics, strikes, embargoes or unusually severe weather. Dates or time of performance shall be extended to the extent of delays excused by this section provided that the party whose performance is affected notifies the other promptly of the existence and nature of such delay.

23. **Notices:** Unless otherwise specified in an attachment hereto, any notice hereunder shall be in writing and addressed to the persons and addresses below.

    To the University:

    University of Maine System
    16 Central Street
    Bangor, Maine 04401

Attn: **John Forker**

To Contractor:

<<BID INSTRUCTIONS – Bidder to supply information noted below for submission with their proposal/bid. >>
Company Name:
Contact Name:
Address:
Phone Number:
Fax Number:

24. **Invoices:** Unless otherwise specified in an attachment hereto, invoices and questions regarding invoices will be directed to:

    Accounts Payable Shared Services
    5765 Service Bldg.
    Orono, ME 04469

    Phone: 207-581-2692 Donita Gallant
    Fax: 207-581-2698
    Email: UMAP@maine.edu

25. **Order of Precedence:** In the event of any conflict among the documents in this agreement, the following order of precedence shall apply:
    A. **Terms and conditions of this Agreement**
    B. **Rider A** - Specifications of Work to be Performed
    C. **Rider A-1** – Pricing
    D. **Rider B-1** – Insurance Requirements
    E. **Rider B-2** – Substitute Form W-9 - Taxpayer Identification Number Request & Certification
    F. **Rider C** – University of Maine System Standards for Safeguarding Information
    G. **Rider D** – Implementation Plan and Timeline
    H. **Rider E** – Service Engagement Form
    I. **Rider F** – Contractor's Service Level Agreement to Support the University
    J. **Contract Amendments** as required
    K. **Request for Proposal #36-15** Dated January 16, 2015 Titled Payment Card Industry (PCI) Data Security Penetration Testing
    L. **Contractor's Bid in Response to Request for Proposal #36-15 Proposal Submission Date** January 28, 2015 **Titled** Payment Card Industry (PCI) Data Security Penetration Testing

26. Multi-Institution Capabilities University will have the option to include products and services under this Agreement to additional University institutions, this includes any additional University institutions formed during the term of this agreement, all facilities utilized by an institution including those managed and/or owned by a third party, and additional entities, such as, the University College a division of University of Maine at Augusta.

The Community College System and Maine Maritime Academy, both public higher education institutions in the state, shall be permitted to piggyback off of the University's contract if they should so desire. The Contractor agrees to further provide the products and services, with all the same terms and conditions applicable, to these additional entities.

27. Signatures

FOR THE UNIVERSITY OF MAINE SYSTEM:

BY: _____
(signature)

Name: _____
(print or type)

Title: _____

Address: _____

_____

_____

_____

Telephone: _____

Fax: _____

Date: _____

FOR THE CONTRACTOR:

LEGAL NAME: _____

BY: _____
(signature)

Name: _____
(print or type)

Title: _____

Address: _____

_____

_____

_____

Telephone: _____

Fax: _____

Date: _____

Tax ID #: _____

Per University policy, "Any contract or agreement for services that will, or may, result in the expenditure by the University of $50,000 or more must be approved in writing by the Chief Procurement Officer, or designee, and it is not approved, valid or effective until such written approval is granted."

BY: _____

Title: _____
Chief Procurement Officer or designee

Date: _____

RIDER A
SPECIFICATIONS OF WORK TO BE PERFORMED

The Contractor agrees to the **Specifications of Work to be Performed** as follows:

INTENT AND PURPOSE
The University of Maine System sought proposals to provide PCI Data Security Standard Penetration Testing. for services of internal/external penetration testing which will meet the minimum requirements as set forth by the PCI DSS SAQ (sections 11.3 and 11.3.4).

PRODUCT SCOPE OF WORK:
<< BID INSTRUCTIONS - Bidder to provide product/service scope of work description as part of their proposal/bid submission. >>

Additional Scope: The Contractor shall permit product and services not covered herein to be added by mutual agreement, without voiding the provisions of the existing contract. The Contractor, for additional consideration, shall furnish additional such products and services to the University.

PRICING: Refer to RIDER A-1

PERFORMANCE TERMS AND CONDITIONS

1. **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 University Contract Administrator notifies the Contractor in writing that any person employed on this Contract is incompetent, disorderly, or otherwise unsatisfactory, such person shall not again be utilized in the execution of this Contract without the prior written consent of the Contract Administrator.

2. **Business and Performance Reviews:** Recognizing that successful performance of this contract is dependent on favorable response, the Contractor shall meet at least quarterly with the Contract Administrator or designee for a business and performance review to evaluate operations and make necessary adjustments. These meetings will normally be conducted electronically but shall be face-to-face on demand. As part of these reviews, the University reserves the right to review equipment specifications quarterly and update equipment specifications accordingly. Contractor shall provide a single point of contact (i.e., relationship manager) and shall notify University in writing and in advance whenever there is a change to that single point of contact.

3. **Campus Visits:** The Contractor agrees to maintain good relations with the University. The Contractor shall make campus visits “as needed” on three days’ notice. The Contractor will coordinate campus visits with the University Services Information and Technology Department to ensure proper communication and sharing of information related to customer projects.

4. **Toll-Free Access**: The Contractor shall provide to the University, toll-free telephone access to technical support. The University prefers a unique toll-free telephone number just for the University. The Contractor shall provide an escalated support feature to ensure

that unresolved support issues can be elevated to upper level management.

5. **Accessibility:** Contractor hereby warrants that the products or services to be provided under this agreement comply with the accessibility guidelines of "Section 508 of the Rehabilitation Act of 1973" as amended as of the date of this agreement, and the "Web Content Accessibility Guidelines (WCAG) 2.0" published by www.w3.org.

   Contractor agrees to promptly respond to and resolve any complaint regarding accessibility of its products or services which is brought to its attention and vendor further agrees to indemnify and hold harmless the University of Maine campuses and system or any university entity using the Contractor's products or services from any claim arising out of its failure to comply with the aforesaid requirements.

   The University, at its discretion, may at any time test the vendor's products or services covered by this agreement to ensure compliance with Section 508 and WCAG 2.0. Testing that results in findings of non-compliance, shall result in a 25% reduction in the total cost of the products and/or services covered by this agreement if the non-compliance is not corrected within 30 days of being reported to the vendor in writing. All withheld amounts will be paid to the vendor upon correction of the non-compliance and acceptance by the University. Said acceptance not to be unreasonably withheld.

   Failure to comply with these requirements shall constitute a breach and be grounds for termination of this agreement and a pro-rated refund of fees paid from the University for the remainder of original contract period.

6. **Standards for Safeguarding Information:** The Contractor is expected to comply with these standards as outlined in ***Attachment C - University of Maine System Standards for Safeguarding Information***. Should the Contractor fail to comply with the standards and is unable to reasonably cure its noncompliance within 60 days, the University may terminate this agreement. The University will be entitled to receive a prorated refund measured from the effective date of the termination.

7. **Implementation Plan and Timeline:** The Contractor is expected to develop, manage and report the status of the progress on the implementation plan and timeline as outlined in ***Attachment D – Implementation Plan and Timeline***, of this Agreement.

8. **Service Level Agreement:** The Contractor is expected to provide, monitor performance and provide reports of its service delivery commitments to the University as outlined in ***Attachment F – Contractor's Service Level Agreement to Support the University***, of this Agreement.

RIDER A-1
PRICING

<< BID INSTRUCTIONS - Details in Exhibit 1 will be inserted here during Agreement negotiations. No action needed for Bidder as part of their proposal/bid submission. >>

RIDER B-1
INSURANCE REQUIREMENTS

<< BID INSTRUCTIONS - Bidder to provide their Contractor's Liability Insurance (CIA) Form here as part of their proposal/bid submission. The text below will be removed and the CIA form will be inserted as an image under Rider B-1>>

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 (In Compliance with Maine Law)	Required for all personnel

Coverage limit requirements can be met with a single underlying insurance policy or through the combination of an underlying insurance policy plus an Umbrella insurance policy.

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.

The University reserves the right to change the insurance requirement or to approve alternative insurances or limits, at the University's discretion.

RIDER B-2

Substitute Form W-9 - Taxpayer Identification Number Request & Certification

Please complete the following information. We are required by law to obtain this information from you when making a reportable payment to you. If you do not provide us with this information, your payments may be subject to federal income tax backup withholding. Use this form only if you are a **U.S. person** (including US. resident alien.). If you are a foreign person, use the appropriate Form W-8.

Part 1 Tax Status:

Print Name: _____

Address (number, street, and apt. or suite no.):_____

City: _____ State: _____ Zip: _____

Phone: (____)_____

Complete One:

☐ Individual/Sole Proprietor Business Name, if different from above _____

Social Security Number __ __ __ - __ __ -__ __ __ __

- or - Business EIN __ __ - __ __ __ __ __ __ __

☐ Partnership EIN __ __ - __ __ __ __ __ __ __

☐ Corporation EIN __ __ - __ __ __ __ __ __ __

Please answer questions below if you are a corporation:

1. Corporation providing legal services? **Y** **N**
2. Corporation providing medical services? **Y** **N**

☐ Limited Liability Company EIN __ __ - __ __ __ __ __ __ __

☐ Tax-Exempt or Not-for-Profit under § 501(C)(3) EIN __ __ - __ __ __ __ __ __ __

☐ Government Entity EIN __ __ - __ __ __ __ __ __ __

☐ Estate or Trust EIN __ __ - __ __ __ __ __ __ __

☐ All other Entities EIN __ __ - __ __ __ __ __ __ __

Part 2 Exemption: **If exempt from Form 1099 reporting, check here:** ☐
and circle your qualifying exemption reason below

1. An organization exempt from tax under IRC section 501(a)
2. The United States or any of its agencies or instrumentalities
3. A state, the District of Columbia, a possession of the United States, or any of their political subdivisions or instrumentalities
4. A foreign government or any of its political subdivisions, agencies, or instrumentalities
5. An international organization or any of its agencies or instrumentalities
6. Other: _____

Part 3 Certification:

Under penalties of perjury, I certify that:

1. The number shown on this form is my correct taxpayer identification number (or I am waiting for a number to be issued to me), **and**
2. I am not subject to backup withholding because: (a) I am exempt from backup withholding, or **(b)** I have not been notified by the Internal Revenue Service (IRS) that I am subject to backup withholding as a result of a failure to report all interest or dividends, or **(c)** the IRS has notified me that I am no longer subject to backup withholding,

and

3. I am a U.S. person (including a U.S. resident alien).

Certification instructions. You must cross out item 2 above if you have been notified by the IRS that you are currently subject to backup withholding because you have failed to report all interest and dividends on your tax return.

Signature of U.S. person: _____Date: _____

Please return this form with the attached contract. Thank you for your cooperation.

RIDER C
UNIVERSITY OF MAINE SYSTEM
STANDARDS FOR SAFEGUARDING INFORMATION

This Attachment addresses the Contractor's responsibility for safeguarding Compliant Data and Business Sensitive Information consistent with the University of Maine System's Information Security Policy and Standards. (infosecurity.maine.edu)

Compliant Data is defined as data that the University needs to protect in accordance with statute, contract, law or agreement. Examples include Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA), Maine Notice of Risk to Personal Data Act, and the Payment Card Industry Data Security Standards (PCI-DSS).

Business Sensitive Information is defined as data which is not subject to statutory or contractual obligations but where the compromise or exposure of the information could result in damage or loss to the University.

1. Standards for Safeguarding Information: The Contractor agrees to implement reasonable and appropriate security measures to protect all systems that transmit, store or process Compliant Data and Business Sensitive Information or personally identifiable information from Compliant Data and Business Sensitive Information furnished by the University, or collected by the Contractor on behalf of the University, against loss of data, unauthorized use or disclosure, and take measures to adequately protect against unauthorized access and malware in the course of this engagement.

   A. Compliant Data and Business Sensitive Information may include, but is not limited to names, addresses, phone numbers, financial information, bank account and credit card numbers, other employee and student personal information (including their academic record, etc.), Driver's License and Social Security numbers, in both paper and electronic format.

   B. If information pertaining to student educational records is accessed, transferred, stored or processed by Contractor; Contractor shall protect such data in accordance with FERPA.

   C. If information pertaining to protected health information is accessed, used, collected, transferred, stored or processed by Contractor; Contractor shall protect such data in accordance with HIPAA and Contractor shall sign and adhere to a Business Associate Agreement.

   D. If Contractor engages in electronic commerce on behalf of the University or cardholder data relating to University activities is accessed, transferred, stored or processed by Contractor; Contractor shall protect such data in accordance with current PCI-DSS guidelines.

   E. If information pertaining to protected "Customer Financial Information" is accessed, transferred, stored or processed by Contractor; Contractor shall protect such data in accordance with GLBA.

2. Prohibition of Unauthorized Use or Disclosure of Information: Contractor agrees to hold all information in strict confidence. Contractor shall not use or disclose information received from,

or created or received by, Contractor on behalf of the University except as permitted or required by this Agreement, as required by law, or as otherwise authorized in writing by the University.

3. Return or Destruction of Compliant or Business Sensitive Information:

   A. Except as provided in Section 3(B), upon termination, cancellation, or expiration of the Agreement, for any reason, Contractor shall cease and desist all uses and disclosures of Compliant Data or Business Sensitive Information and shall immediately return or destroy (if the University gives written permission to destroy) in a reasonable manner all such information received from the University, or created or received by Contractor on behalf of the University, provided, however, that Contractor shall reasonably cooperate with the University to ensure that no original information records are destroyed. This provision shall apply to information that is in the possession of subcontractors or agents of Contractor. Contractor shall retain no copies of University information, including any compilations derived from and allowing identification of any individual's confidential information. Except as provided in Section 3(B), Contractor shall return (or destroy) information within 30 days after termination, cancellation, or expiration of this Agreement.

   B. In the event that Contractor determines that returning or destroying any such information is infeasible, Contractor shall provide to University notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the Parties that return or destruction of such information is infeasible, Contractor shall extend the protections of this Agreement to such information and limit further uses and disclosures of such information to those purposes that make the return or destruction infeasible, for so long as Contractor maintains such information.

   C. Contractor shall wipe or securely delete Compliant Data or Business Sensitive Information and personally identifiable information furnished by the University from storage media when no longer needed. Measures taken shall be commensurate with the standard for "clearing" as specified in the National Institute of Standards and Technology (NIST) Special Publication SP800-88: Guidelines for Media Sanitization, prior to disposal or reuse.

4. Term and Termination:

   A. This Attachment shall take effect upon execution and shall be in effect commensurate with the term of the Agreement

5. Subcontractors and Agents: If Contractor provides any Compliant Data or Business Sensitive Information received from the University, or created or received by Contractor on behalf of the University, to a subcontractor or agent, the Contractor shall require such subcontractor or agent to agree to the same restrictions and conditions as are imposed on Contractor by this Agreement.

6. Contractor shall control access to University data: All Contractor employees shall be adequately screened, commensurate with the sensitivity of their jobs. Contractor agrees to limit employee access to data on a need-to-know basis. Contractor shall impose a disciplinary process for employees not following privacy procedures. Contractor shall have a process to remove access to University data immediately upon termination or re-assignment of an employee by the Contractor.

7. Unless otherwise stated in the agreement, all Compliant Data or Business Sensitive Information is the property of the University and shall be turned over to the University upon request.

8. Contractor shall not amend or replace University-owned hardware, software or data without prior authorization of the University.

9. If mobile devices are used in the performance of this Agreement to access University Compliant Data or Business Sensitive Information, Contractor shall install and activate authentication and encryption capabilities on each mobile device in use.

10. Reporting of Unauthorized Disclosures or Misuse of Information: Contractor shall report to the University any use or disclosure of Compliant Data or Business Sensitive Information not authorized by this Agreement or in writing by the University. Contractor shall make the report to the University not more than one (1) business day after Contractor learns of such use or disclosure. Contractor's report shall identify; (i) the nature of the unauthorized use or disclosure, (ii) the information used or disclosed, (iii) who made the unauthorized use or received the unauthorized disclosure, (iv) what Contractor has done or shall do to mitigate the effects of the unauthorized use or disclosure, and (v) what corrective action Contractor has taken or shall take to prevent future similar unauthorized use or disclosure. Contractor shall provide such other information, including a written report, as reasonably requested by the University. Contractor shall keep University informed on the progress of each step of the incident response. Contractor shall indemnify and hold University harmless from all liabilities, costs and damages arising out of or in any manner connected with the security breach or unauthorized use or disclosure by Contractor of any University Compliant Data or Business Sensitive Information. Contractor shall mitigate, to the extent practicable, any harmful effect that is known to Contractor of a security breach or use or disclosure of Compliant Data or Business Sensitive Information by Contractor in violation of the requirements of this Agreement. In addition to the rights of the Parties established by this Agreement, if the University reasonably determines in good faith that Contractor has materially breached any of its obligations, the University, in its sole discretion, shall have the right to:

    - Inspect the data that has not been safeguarded and thus has resulted in the material breach, and/or
    - Require Contractor to submit a plan of monitoring and reporting, as the University may determine necessary to maintain compliance with this Agreement; and/or Terminate the Agreement immediately.

11. Survival: The respective rights and obligations of Contractor under Section 12 of the Agreement or Section 3 of this Attachment shall survive the termination of this Agreement.

12. Contractor Hosted Data: If Contractor hosts University Compliant Data or Business Sensitive Data, in or on Contractor facilities, the following clauses apply.

    A. Contactor computers that host University Compliant Data or Business Sensitive Information shall be housed in secure areas that have adequate walls and entry control such as a card controlled entry or staffed reception desk. Only authorized personnel shall be allowed to enter and visitor entry will be strictly controlled.

B. Contractor shall design and apply physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disasters. Contractor shall protect hosted systems with Uninterruptible Power Supply (UPS) devices sufficient to meet business continuity requirements.

C. Contractor shall backup systems or media stored at a separate location with incremental back-ups at least daily and full back-ups at least weekly. Incremental and full back-ups shall be retained for 15 days and 45 days respectively. Contractor shall test restore procedures not less than once per year.

D. Contractor shall provide for reasonable and adequate protection on its network and system to include firewall and intrusion detection/prevention.

E. Contractor shall use strong encryption and certificate-based authentication on any server hosting on-line and e-commerce transactions with the University to ensure the confidentiality and non-repudiation of the transaction while crossing networks.

F. The installation or modification of software on systems containing University Compliant Data or Business Sensitive Information shall be subject to formal change management procedures and segregation of duties requirements.

G. Contractor who hosts University Compliant Data or Business Sensitive Information shall engage an independent third-party auditor to evaluate the information security controls not less than every two (2) years. Such evaluations shall be made available to the University upon request.

H. Contractor shall require strong passwords for any user accessing personally identifiable information or data covered under law, regulation, or standard such as HIPAA, FERPA, or PCI. Strong passwords shall be at least eight characters long; contain at least one upper and one lower case alphabetic characters; and contain at least one numeric or special character.

13. If the Contractor provides system development, Compliant Data or Business Sensitive Information shall not be used in the development or test environments. Records that contain these types of data elements may be used if that data is first de-identified, masked or altered so that the original value is not recoverable. For programs that process University data, initial implementation as well as applied updates and modifications must be produced from specifically authorized and trusted program source libraries and personnel. Contractor shall provide documentation of a risk assessment of new system development or changes to a system.

RIDER D
IMPLEMENTATION PLAN AND TIMELINE

<<BID INSTRUCTIONS – Bidders will insert their implementation plan and timeline here as part of their proposal/bid submission. >>

RIDER E
SERVICES ENGAGEMENT FORM

Services Engagement to Agreement for Services

This Services Engagement is entered into as of the date written below between _____ ("Contractor") and _____ ("Institution").

This Services Engagement shall be governed by the terms and conditions of the Master Level Agreement for Services dated _____ by and between _____ ("Contractor") and the University of Maine System, and is incorporated herein by reference.

This Services Engagement describes the Services to be provided by _____ ("Contractor") and the fees associated with such Services.

INSTITUTION REPRESENTATIVE & PROJECT MANAGER:

CONTRACTOR REPRESENTATIVE & PROJECT MANAGER:

SCOPE OF WORK:

TERM:
The term of this Work Order will be from _____ to _____.

PRICE:

SIGNATURES:

Institution	**Contractor**
By: _____	By: _____
Name: _____	Name: _____
Title: _____	Title: _____
Date: _____	Date: _____

RIDER F
CONTRACTOR'S SERVICE LEVEL AGREEMENT TO SUPPORT THE UNIVERSITY

<<BID INSTRUCTIONS – Bidders will insert their Service Level Agreement (SLA) here as part of their proposal/bid submission. >>