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

Payment Card Industry (PCI) Data Security Penetration Testing

RFP #2020-017

Issued Date: December 3, 2019

Response Deadline Date/Time: December 13, 2019 11:59 p.m. EST

Response Submission Information:

Submitted electronically to robin.cyr@maine.edu
Email Subject Line – RC – PCI Data Security Penetration Testing - RFP#2020-017

Response Contact Information:

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

Table of Contents

1.0 INTRODUCTION

1.1 Definitions, Background, Purpose and Specifications

1.1.1 Definitions

The University of Maine System will hereinafter be referred to as the "University." Respondents to the document shall be referred to as "Respondent(s)" or "Respondent".

The Respondent to whom the Agreement is awarded shall be referred to as the "Contractor."

The University of Maine System and other components of the University shall be referred to as "Multi-Institution".

1.1.2 Background

Overview

Established in 1968, the University of Maine System (UMS) unites seven distinctive public universities, comprising 10 campuses and numerous centers, in the common purposes of providing quality higher education while delivering on its traditional tripartite mission of teaching, research, and public service.

Maine's largest educational enterprise, the University extends its mission as a major resource for the state, linking economic growth, the education of its people, and the application of research and scholarship.

A comprehensive public institution of higher education, UMS serves nearly 40,000 students annually and is supported by the efforts of more than 2,000 full-time and part-time faculty, more than 3,000 regular full-time and part-time staff, and a complement of part-time temporary (adjunct) faculty.

Reaching more than 500,000 people annually through educational and cultural offerings, the University of Maine System also benefits from more than two-thirds of its alumni population residing within the state; more than 123,000 individuals.

The System consists of the following seven universities: University of Maine (UM); University of Maine at Machias (UMM); University of Maine at Augusta (UMA); University of Maine at Presque Isle (UMPI); University of Maine at Farmington (UMF); University of Southern Maine (USM); and, University of Maine at Fort Kent (UMFK).

Operating within a shared services model, the offices of Information Technology, Strategic Procurement, Human Resources, Facilities, Risk and General Services, Finance and Budget, Shared Processing Center, General Counsel and Organizational Effectiveness partner to form the University Services organization.

Charged with delivering key administrative functions across the System, University Services is dedicated to leveraging its significant unit and collective resources to not only serve the immediate needs of its constituents, but deliver sustainable economies and efficiencies for the future benefit of the System as well.

Campus thumbnails

University of Maine at Augusta

Founded in 1965, the University of Maine at Augusta transforms the lives of students of every age and background across the State of Maine and beyond through access to high-quality distance and on-site education, excellence in student support, civic engagement, and professional and liberal arts programs. Celebrating its 50th anniversary, UMA is the third largest public university in Maine. In addition to its main campus in the state's capital, UMA also serves students at its campus in Bangor (UMA Bangor) and through University College centers around the state. With its multiple locations and long-term expertise in online and distance learning, UMA is generally considered the university of choice for Mainers of all ages who want to attend college without uprooting their lives.

University of Maine at Farmington

Established in 1864, the University of Maine at Farmington is a small, increasingly selective public liberal arts college, featuring programs in teacher education, the arts & sciences and professional studies, serving primarily full-time, traditional-age undergraduates in a residential setting. Farmington continues to be recognized for its academic quality, small classes, close-knit community and integrated curricular, co-curricular and extra-curricular offerings. With enrollment at around 1,800 full-time students, UMF is about the same size as many of New England's most selective private colleges and offers many of the same advantages, yet at a very attractive price.

University of Maine at Fort Kent

Founded in 1878, the University of Maine at Fort Kent is a unique learning institution perfect for people seeking a rural scholastic atmosphere of modern academic standards combined with an eclectic mix of rugged outdoor vistas and access to cosmopolitan epicenters across two countries. The learning opportunities at UMFK have become a model of a "rural university" that other New England campuses attempt to emulate. Strong academic programs include associate and bachelor's degrees in such disciplines as nursing, business, education, forestry and cyber security among others. The student body at UMFK numbering 1,500, has a higher percentage of international students than any other university in New England, allowing immersion in a cultural opportunity that is unique in the world. Featuring seventy-seven full-time and adjunct faculty and eighty-one staff, UMFK enjoys national recognition for quality and value as well as championships in men's and women's soccer.

University of Maine at Machias

The University of Maine at Machias, a member of the University of Maine System, sits on the Gulf of Maine, surrounded by rivers, forests, fishing villages, and blueberry barrens. This unspoiled portion of the Atlantic coast is known for its outdoor recreational opportunities and quality of life. As Maine's Coastal University, faculty and students approach the liberal arts with a focus on coastal, environmental and community issues. The academic experience emphasizes learning both in the classroom and in experiential settings. UMM's fifteen undergraduate degree programs serve approximately 800 students. The University's applied research and public services contribute to the improvement of the quality of life and economic development in Downeast Maine.

University of Maine

Established as a land grant college in 1865, the University of Maine is a public research university located in Orono and referred to as the flagship institution of the University of Maine System. UMaine, as it is often called, has an overall enrollment of over 11,000 students who pursue majors in ninety undergraduate disciplines, more than seventy masters' courses of study and thirty doctoral programs. Ranked 105th by the National Science Foundation among American research universities, UMaine's research faculty has an international reputation for excellence and the campus' Fogler Library is the largest in the state. Located on more than 600 acres only a few miles from Bangor, one of Maine's largest cities, the University of Maine is a major resource not only for education but economic and community development throughout the state as well.

University of Maine at Presque Isle

For more than a century, the University of Maine at Presque Isle has been helping students find their path to great professional careers providing its 1,100 traditional and non-traditional students from all areas of the state, country, and world with life-changing opportunities in a caring, small-university environment. UMPI combines liberal arts and selected professional programs and serves as a cultural and educational resource for the entire region. The campus sits on 150 acres surrounded by the rolling hills and potato fields of northern Maine and the University strives to be the region's premier learning institution while helping to stimulate cultural and economic development in Aroostook County and the State of Maine. The University serves as an educational and cultural center for the area and its facilities are utilized for lectures, programs, concerts, dance performances, exhibits, and plays that benefit the entire region.

University of Southern Maine

The University of Southern Maine, northern New England's outstanding public, regional, comprehensive university, is dedicated to providing its diverse student body of more than 9,000 students from forty states and thirty foreign countries with a high-quality, accessible, affordable education. Through its undergraduate, graduate, and professional programs, USM faculty members educate future leaders in the liberal arts and sciences, engineering and technology, health and social services, education, business, law, and public service. Located on three campuses in Gorham, Portland, and Lewiston-Auburn, USM is known as Maine's Metropolitan University and serves communities that are among the largest population centers in the state.

1.1.3 Purpose

This document provides instructions for submitting responses, the procedure and criteria by which the Respondent(s) will be selected, and the contractual terms which will govern the relationship between the University and the awarded Respondent(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).

Respondents should review **1.1.4 Specifications / Scope of Work** of this document to see the full Scope of Services/Products required.

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.

1.1.4 Specifications / Scope of Work

Penetration testing will include internal and external testing on network devices residing at University of Maine System Institutions. Bidders may choose to travel to campus locations at their discretion to provide their most effective penetration testing services.

Level I Penetration Testing Deliverables - Penetration testing for each Institution will require testing for the payment devices identified. Penetration testing will meet the minimum requirements of **PCI DSS 3.2.1 (section 11.3),** 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.
    a. Application-layer penetration tests (where applicable) that include the vulnerabilities noted in the **PCI DSS 3.2.1 Requirements (Sections 6.5.1 - 6.5.10).** 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 targeted penetration testing for a web application or system that supports the payment environment. Such requirements will include testing of vulnerabilities described in current OWASP, or similar, security guidance and those noted in the **PCI DSS 3.2.1 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.

Level III - UMS Institutions may need additional penetration testing services to confirm alignment with other security or compliance frameworks (e.g. NIST-800 171). The scope (e.g. numbers of systems and networks) and complexity of such tests will be determined by consultation with the system owner for the specific compliance need. Offerings should include testing at various levels, to include at a minimum:

- 1. Confirmation of proper network segmentation
- 2. Identification and validation of vulnerabilities of network facing services
- 3. Leveraging detected vulnerabilities for lateral movement within sets of identified systems
- 4. Application-specific testing, to include Web Application testing, to identify at a minimum OWASP Top 10 vulnerabilities.

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 jointly develop 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.

An estimate of Year 1 scheduled activities is detailed in the table directly below and will form the deliverables required for the first Service Engagement form. Counts and locations are subject to change due to ongoing updates that could affect the need to pentest specific cardholder environments. 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	75	Level I	January 15, 2020
2	University of Maine at Farmington	Farmington. Maine	10	Level I	January 15, 2020
3	University of Southern Maine	Portland, Maine	10	Level I	January 15, 2020
4	University of Maine at Augusta	Augusta. Maine	10	Level I	January 15, 2020
5	University of Maine at Fort Kent	Fort Kent, Maine	3	Level I	January 15, 2020
6	University of Maine at Machias	Machias, Maine	3	Level I	January 15, 2020
7	University of Maine at Presque Isle	Presque Isle, Maine	2	Level I	January 15, 2020

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.

1.2 General Information

1.2.1 Contract Administration and Conditions

1.2.1.1 The winning Respondent will be required to execute a contract in the form of a University of Maine System Contract for Services, which is attached to this response as **Appendix E**. Contract initial term and renewal periods are reflected in Section 2 of Appendix E, Contract for Services, and are subject to continued availability of funding and satisfactory performance.

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

In the event of a conflict of terms the following precedence will apply:

1. University of Maine System Contract for Services
2. Agreement Riders as required
3. Contract Amendments (as required)
4. The University's RFP
5. Respondent's Submission
6. Purchase Order or Letter of Agreement

1.2.1.2 Modification of Agreement terms and conditions is permitted except that the University, due to its public nature, will not :

a. Provide any defense, hold harmless or indemnity;
b. Waive any statutory or constitutional immunity;
c. Apply the law of a state other than Maine;
d. Procure types or amounts of insurance beyond those UMS already maintains or waive any rights of subrogation.
e. Add any entity as an additional insured to UMS policies of insurance;
f. Pay attorneys' fees, costs, expenses or liquidated damages;
g. Promise confidentiality in a manner contrary to Maine's Freedom of Access Act;
h. Permit an entity to change unilaterally any term or condition once the contract is signed;
i. Accept any references to terms and conditions, privacy policies or any other websites, documents or conditions referenced outside of the contract; or
j. Agree to automatic renewals for term(s) greater than month-to-month.

1.2.1.3 By submitting a response to a Request for Proposal, bid or other offer to do business with the University your entity understands and agrees that:

a. The above Agreement provisions **(Section 1.2.1.2)** will not be modified and are thereby incorporated into any agreement entered into between University and your entity; that such terms and condition shall control in the event of any conflict with such agreement; and that your entity will not propose or demand any contrary terms;
b. The above Agreement provisions **(Section 1.2.1.2)** will govern the interpretation of such agreement notwithstanding the expression of any other term and/or condition to the contrary;
c. Your entity agrees that the resulting Agreement will be the entire agreement between the University (including University's employees and other End Users) and Respondent and in the event that the Respondent requires terms of use agreements or other agreements, policies or understanding, whether on an order form, invoice, website, electronic, click-through, verbal or in writing, with University's employees or other End Users, such agreements shall be null, void and without effect, and the terms of the Agreement shall apply.
d. Your entity will identify at the time of submission which, if any, portion or your submitted materials are entitled to "trade secret" exemption from disclosure under Maine's Freedom of Access Act; that failure to so identify will authorize UMS to conclude that no portions are so exempt; and that your entity will defend, indemnify and hold harmless UMS in any and all legal actions that seek to compel UMS to disclose under Maine's Freedom of Access Act some or all of your submitted materials and/or contract, if any, executed between UMS and your entity.

1.2.2 Communication with the University

It is the responsibility of the Respondent to inquire about any requirement of this document that is not understood. Responses to inquiries, if they change or clarify the document in a substantial manner, will be forwarded by addenda to all parties that have received a copy of the document. Addenda will also be posted on our web site, **www.maine.edu/strategic/upcoming_bids.php**

It is the responsibility of all Respondents 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 using the **Response Contact Information** provided on the cover sheet of this document. Refer to table in **Section 1.3.1 Timeline of Key Events** for deadline requirements.

1.2.3 Confidentiality

The University must adhere to the provisions of the Maine Freedom of Access Act (FOAA), 1 MRSA §401 et seq. As a condition of submitting a response under this

section, a respondent 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.

The information contained in responses submitted for the University's consideration will be held in confidence until all evaluations are concluded and a Respondent selected (the successful Respondent). At that time the University will issue award notice letters to all participating Respondents and all Respondents' responses may be made available to participating Respondents upon request. Such request must be made by submitting a written request to the individual noted in the Response Contact Information shown on the cover sheet of this document, with a copy of the request provided to the other Respondents. Such requests are public records.

After the protest period has passed and the Agreement is fully executed, responses will be available for public inspection upon request.

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 that meets the definition of "trade secret" under Maine law. Clearly mark any portion of your submitted materials which are entitled to "trade secret" exemption from disclosure under Maine's Freedom of Access Act. Failure to so identify as trade secret will authorize the University to conclude that no portions are so exempt; and that your entity will defend, indemnify and hold harmless the University in any and all legal actions that seek to compel the University to disclose under Maine's Freedom of Access Act some or all of your submitted materials and/or contract, if any, executed between the University and your entity.

1.2.4 Costs of Preparation

Respondent assumes all costs of preparation of the response and any presentations necessary to the response process.

1.2.5 Authorization

Any 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.

1.2.6 Multi-Institutional

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

1.2.7 Pricing

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

1.2.8 Cost Response Form Quantities

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

1.2.9 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 Agreement Administrator or designee, notifies the Contractor in writing that any person employed on this Agreement is incompetent, disorderly, or otherwise unsatisfactory, such person shall not again be employed in the execution of this Agreement without the prior written consent of the Agreement Administrator.

1.2.10 Environment Compliance

In the event that the resulting Agreement involves the generation, transportation, handling, disposal, and/or other operations or activities in relation to toxic, hazardous, radioactive, or otherwise dangerous gases, vapors, fumes, acids, alkali's, chemicals, wastes or contaminants and/or other substance, material or condition, the Contractor agrees to indemnify save harmless and defend the University from and against all liabilities, claims, damages, forfeitures, suits, and the costs and expenses incident thereto (including costs of defense, settlement and reasonable attorney's fees) which the University may hereafter incur as a result of death or bodily injuries or damage to any property, contamination of or adverse effects of the environment or any violation of state or federal regulations or laws (including without limitation the Resources Conservation and Recovery Act, the Hazardous Material Transportation Act or the Superfund Amendment and Reauthorization Act, as the same now exists or may hereafter be amended) or order based on or arising in whole or in part from the Contractor's performance under the Agreement, provided, however the Contractor shall not indemnify the University for any liabilities, claims, damages, (as set forth above) caused by or arising out of the sole negligence of the University, or arising out of any area of responsibility not attributable to Contractor.

1.2.11 Specification Protest Process and Remedies:

If a Respondent feels that the specifications are written in a way that limits competition, a specification protest may be sent to the Office of Strategic Procurement to the email address provided on the cover page of this document. 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 Deadline for Proposal Submission noted in Section 1.3.1. 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.

1.3 General Submission Provisions

1.3.1 Timeline of Key Events

Reference Section	Event Name	Event Due Date
Section 1.2.2	Deadline for Written Inquiries/Questions	December 6, 2019 5:00 pm EST
Section 1.2.2	Response to Written Inquiries/Questions	December 9, 2019
Section 1.2.2	Deadline for Proposal Submission	December 13, 2019 11:59 pm EST
Section 2.2	Award Announcement **(subject to change)**	December 19, 2019
	Estimated Agreement Start Date **(subject to change)**	January 1, 2020

1.3.2 Eligibility to Submit Responses

Public entities, private for-profit companies, and non-profit companies and institutions are invited to submit a response to this document.

1.3.3 Debarment

Respondents must complete and submit the "Debarment, Performance and Non-Collusion Certification Form provided in Appendix B. Failure to provide this certification may result in the disqualification of the Respondent's proposal, at the University's discretion.

Submission of a signed response 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.

1.3.4 Response Understanding

By submitting a response, the Respondent agrees and assures that the specifications are adequate, and the Respondent accepts the terms and conditions herein. Any exceptions should be noted in your response.

1.3.5 Response Validity

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

1.3.6 Non-Response Submission

The University will not consider non-responsive submissions, i.e., those with material deficiencies, omissions, errors or inconsistencies or that otherwise do not follow instructions. The University in its sole discretion will determine what is Non-Responsive.

1.3.7 Respondents' Presentations

Presentations may be requested of two or more Respondents deemed by the University to be the best suited among those submitting responses on the basis of the selection criteria. After presentations have been conducted, the University may select the Respondent(s) which, in its opinion, has made the response that is the most responsive and most responsible and may award the Agreement to that/those Respondent(s).

1.3.8 Response Submission

A **SIGNED** virus-free electronic copy must be submitted as follows:

- The response must be received electronically to the E-Mail shown in the **Response Submission Information** section of the cover page of this document.
- Electronic submission must be received by the required **Response Deadline Date/Time** reflected on the cover page of this document.
- Response submissions that exceed 20 MB will be submitted with multiple emails modifying email subject line shown in the **Response Submission Information** section of the cover page of this document to include: Submission 1 of X ('X' representing the number of files being submitted).

2.0 EVALUATION AND AWARD PROCESS

2.1 Evaluation Criteria

2.1.1 Scoring Weights

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

Evaluation Appendices	Category	Points
Appendix C	Cost Evaluation	30
Appendix D & E	Contract for Services	10
Appendix F & G	Organization, Qualifications, Experience and References	15
Appendix H	Information Technology	45
	Total Points	**100**

2.1.2 Scoring Section Descriptions

2.1.2.1 Cost Evaluation

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

The scoring formula is:

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

The University will NOT seek a best and final offer (BAFO) from any Respondent in this procurement process. All Respondents are expected to provide their best value pricing with the submission of their response. Respondents will NOT be given another opportunity to modify pricing once submitted.

2.1.2.2 Contract for Services (Appendix D & E)

The evaluation team will use a consensus approach to evaluate and assign evaluation based on pass/fail decision based on University risk assessment. The University reserves the right to reject any or all responses, in whole or in part, for any response receiving no points in this section in accordance with Section 2.2 Award.

Responses will be evaluated using the following guidelines:

a. Full acceptance of the terms and conditions with the Respondents signature on the Agreement signature page, will receive the total points noted in Table 2.1.1.
b. Revisions to the Agreement provisions specified in Section 1.2.1.2 will receive point reductions based on the University's risk assessment.

c. Revisions to the Agreement provisions other than those specified in Section 1.2.1.2 will be evaluated at the University's discretion based on the University's risk assessment.

2.1.2.3 Organization, Qualifications, Experience and References

The evaluation team will use a consensus approach to evaluate and assign evaluation points. Reference checks will be performed on the top Respondent(s) only as determined by consensus scoring in the other categories.

2.1.2.4 Information Technology

The evaluation team will use a consensus approach to evaluate and assign evaluation points.

2.2 Award

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 Agreement(s) to one or multiple Respondents, which may include awards to Respondents for a geographical area, if such award is in the best interest of the University.

The University reserves the right to waive minor irregularities, which may include contacting the Respondent to resolve the irregularity. Scholarships, donations, or gifts to the University, will not be considered in the evaluation of responses. The University reserves the right to reject any or all responses, in whole or in part, and is not necessarily bound to accept the lowest cost response if that response is contrary to the best interests of the University. The University may cancel this request or reject any or all responses in whole or in part. Should the University determine in its sole discretion that only one Respondent is fully qualified, or that one Respondent is clearly more qualified than any other under consideration, an Agreement may be awarded to that Respondent without further action.

2.3 Negotiations

The University reserves the right to negotiate with the successful Respondent to finalize a contract. Such negotiations may not significantly vary the content, nature or requirements of the proposal or the University's Request for Proposals to an extent that may affect the price of goods or services requested. The University reserves the right to terminate contract negotiations with a selected respondent who submits a proposed contract significantly different from the response they submitted in response to the advertised RFP. In the event that an acceptable contract cannot be negotiated with the highest ranked Respondent, the University may withdraw its award and negotiate with the next-highest ranked Respondent, and so on, until an acceptable contract has been finalized. Alternatively, the University may cancel the RFP, at its sole discretion.

2.4 Award Protest

Respondents may appeal the award decision by submitting a written protest to the University of Maine System's Chief General Services Officer within five (5) business days of the date of the award notice, with a copy of the protest to the successful Respondent. The protest must contain a statement of the basis for the challenge. Further information regarding the appeal process can be found at

http://staticweb.maine.edu/wp-content/uploads/2015/07/APL_VII-A_20150630-FINAL.pdf?565a1d

If this RFP results in the creation of a pre-qualified or pre-approved list of vendors, then the appeal procedures mentioned above are available upon the original determination of that vendor list, but not during subsequent competitive procedures involving only the pre-qualified or pre-approved list participants.

3.0 RESPONSE FORMAT REQUIREMENTS

3.1 General Format Instructions

3.1.1 Electronic Submissions

Documents submitted as part of the electronic response are to be prepared on standard electronic formats of 8-1/2" x 11" and of PDF file type. Submissions requiring additional supporting information, such as, foldouts containing charts, spreadsheets, and oversize exhibits are permissible and must be submitted as Appendices, clearly numbered and referencing the Section in which they provide supporting information.

For clarity, the Respondent's name should appear on every document page, including Appendices. Each Appendix must reference the section or subsection number to which it corresponds.

3.1.2 Respondents Responsibility

It is the responsibility of the Respondent to provide all information requested in the document package at the time of submission. Failure to provide information requested in this document 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 response being disqualified for consideration. 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.

3.1.3 Brief Response

Respondents are asked to be brief and to respond to each question listed in the "Response to Questions" section of this document. Number each response in the response to correspond to the relevant question in this document.

3.1.4 Additional Attachments Prohibited

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

3.2 Response Format Instructions

This section contains instructions for Respondents to use in preparing their response. The Respondent's submission must follow the outline used below, including the numbering of section and sub-section headings. Failure to use the outline specified in this section or to respond to all questions and instructions throughout this document may result in the response being disqualified as non-responsive or receiving a reduced score.

The University and its evaluation team for this document have sole discretion to determine whether a variance from the document specifications should result in either disqualification or reduction in scoring of a response.

Re-phrasing of the content provided in this document will, at best, be considered minimally responsive. The University seeks detailed yet succinct responses that demonstrate the Respondent's experience and ability to perform the requirements specified throughout this document.

3.2.1 Section 1 - Response Cover Page

3.2.1.1 Label this response - Section 1 – UMS Response Cover Page
3.2.1.2 Insert Appendix A – University of Maine System Response Cover Page
3.2.1.3 Insert Appendix B – Debarment, Performance and Non-Collusion Certification

3.2.2 Section 2 - Cost Response

3.2.2.1 Label this response - Section 2 – Cost Evaluation
3.2.2.2 Insert Appendix C – Required Cost Evaluation Exhibits

3.2.3 Section 3 - Contract for Services

3.2.3.1 Label this response - Section 3 – Contract for Services
3.2.3.2 Insert Appendix D – Contract for Services
3.2.3.3 Insert Appendix E – Master Agreement

3.2.4 Section 4 - Response to Questions

3.2.4.1 Label this response - Section 4 – Response to Evaluation Questions & Related Information
3.2.4.2 Insert Appendix F – Organization Reference Form
3.2.4.3 Insert Appendix G – Evaluation Question(s) - Organization, Qualifications and Experience
3.2.4.4 Insert Appendix H – Evaluation Question(s) – Information Technology

Appendix A – University of Maine System Response Cover Page

RFP # 2020-017
PCI Data Security Pen 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:	

1. This pricing structure contained herein will remain firm for a period of 90 days from the date and time of the quote deadline date.
2. 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 Respondent's response.
3. No attempt has been made or will be made by the Respondent to induce any other person or firm to submit or not to submit a response.
4. The undersigned is authorized to enter into contractual obligations on behalf of the above-named organization.
5. By submitting a response to a Request for Proposal, bid or other offer to do business with the University your entity understands and agrees that:
    a. The Agreement provisions in **Section 1.2.1.2** of this document will not be modified and are thereby incorporated into any agreement entered into between University and your entity; that such terms and condition shall control in the event of any conflict with such agreement; and that your entity will not propose or demand any contrary terms;
    b. The above Agreement provisions in **Section 1.2.1.2** of this document will govern the interpretation of such agreement notwithstanding the expression of any other term and/or condition to the contrary;
    c. Your entity agrees that the resulting Agreement will be the entire agreement between the University (including University's employees and other End Users) and Respondent and in the event that the Respondent requires terms of use agreements or other agreements, policies or understanding, whether on an order form, invoice, website, electronic, click-through, verbal or in writing, with University's employees or other End Users, such agreements shall be null, void and without effect, and the terms of the Agreement shall apply.
    d. Your entity will identify at the time of submission which, if any, portion or your submitted materials are entitled to "trade secret" exemption from disclosure under Maine's Freedom of Access Act; that failure to so identify will authorize UMS to conclude that no portions are so exempt; and that your entity will defend, indemnify and hold harmless UMS in any and all legal actions that seek to compel UMS to disclose under Maine's Freedom of Access Act some or all of your submitted materials and/or contract, if any, executed between UMS and your entity.

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

Date: _____

_____ _____

Name and Title (Printed) Authorized Signature

Appendix B – Debarment, Performance and Non-Collusion Certification

University of Maine System
DEBARMENT, PERFORMANCE and NON-COLLUSION CERTIFICATION

RFP # 2020-017
PCI Data Security Pen Testing

By signing this document, I certify to the best of my knowledge and belief that the aforementioned organization, its principals and any subcontractors named in this proposal:

a. Are not presently debarred, suspended, proposed for debarment, and declared ineligible or voluntarily excluded from bidding or working on contracts issued by any governmental agency.
b. Have not within three years of submitting the proposal for this contract been convicted of or had a civil judgment rendered against them for:
    i. Fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing a federal, state or local government transaction or contract.
    ii. Violating Federal or State antitrust statutes or committing embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, or receiving stolen property;
    iii. Are not presently indicted for or otherwise criminally or civilly charged by a governmental entity (Federal, State or Local) with commission of any of the offenses enumerated in paragraph (b) of this certification; and
    iv. Have not within a three (3) year period preceding this proposal had one or more federal, state or local government transactions terminated for cause or default.
c. Have not entered into a prior understanding, agreement, or connection with any corporation, firm, or person submitting a response for the same materials, supplies, equipment, or services and this proposal is in all respects fair and without collusion or fraud. The above mentioned entities understand and agree that collusive bidding is a violation of state and federal law and can result in fines, prison sentences, and civil damage awards.

Failure to provide this certification may result in the disqualification of the Respondent's proposal, at the University's discretion.

Date: _____

_____ _____
Name and Title (Printed) Authorized Signature

Appendix C – Required Cost Evaluation Exhibits

University of Maine System
COST EVALUATION

RFP # 2020-017
PCI Data Security Pen Testing

GENERAL INSTRUCTIONS:

1. The Respondent must submit a cost response that covers the entire period of the Agreement, including any optional renewal periods.

2. The cost response shall include the costs necessary for the Respondent to fully comply with the Agreement terms and conditions and requirements. **Note regarding total cost of ownership:** This "cost" will encompass the entire solution pricing along with all products and services offered as part of the solution.

3. Failure to provide the requested information and to follow the required cost response format provided in Appendix C may result in the exclusion of the Response from consideration, at the discretion of the University. You can add rows and columns required to insert additional information. If a particular cost table is not required as part of your response simply leave it blank.

4. No costs related to the preparation of the Response for this document or to the negotiation of the Agreement with the University may be included in the Response. Only costs to be incurred after the Agreement effective date that are specifically related to the implementation or operation of contracted services may be included.

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

6. If there are additional options or services that are not included in the offering, they must be identified and itemized as "optional" and include a description of the product or service and the costs of the option. All items identified in the response (including third party items required) will be considered free add-ons to the proposed solution at the prices included in this response unless expressly stated otherwise.

7. Respondents' are encouraged to provide additional price incentives for providing an enterprise solution, multi-year or award of multiple institutions.

8. Pricing will be guaranteed by the vendor for the term of the Agreement.

9. The University will NOT seek a best and final offer (BAFO) from any Respondent in this procurement process. All Respondents are expected to provide their best value pricing with the submission of their response. Respondents will NOT be given another opportunity to modify pricing once submitted.

10. An **MS Excel Version** must be included in your final submission for all of these tables. For a copy of the excel version, email the contact provided on the cover page of this document.

INSTRUCTIONS FOR – Exhibit 1 (Table 1) – Penetration Testing Pricing for Section 1.1.4 Scope of Work Table 1 Identified Testing Activities

The Respondent is to submit the cost for the testing activities identified in **Section 1.1.4 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 1.1.4 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 testing can be found in **Section 1.1.4 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) – Respondents will use this attachment to record all costs associated with this section. For a copy of the excel version of Exhibit 1, email the contact provided on the cover page of this document.

#	Institution Name	Location	IP	Testing Type Deliverable	Req Hours	Total Cost
1	University of Maine	Orono, Maine	75	Level I		
2	University of Maine at Farmington	Farmington. Maine	10	Level I		
3	University of Southern Maine	Portland, Maine	10	Level I		
4	University of Maine at Augusta	Augusta. Maine	10	Level I		
5	University of Maine at Fort Kent	Fort Kent, Maine	3	Level I		
6	University of Maine at Machias	Machias, Maine	3	Level I		
7	University of Maine at Presque Isle	Presque Isle, Maine	2	Level I		
	Include additional explanation of costs and list assumptions that could influence the cost of change request pricing.					
	List explanations and assumptions here;					
	-					
	-					
	-					

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

The Respondent is to submit number of hours and hourly rate to complete **Level I Penetration Testing**, as detailed in **Section 1.1.4 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 Respondent costing model includes other factors in calculation of cost, such as number of IPs, than the Respondent 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 1.1.4 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 2) – Respondents will use this attachment to record all costs associated with this section. For a copy of the excel version of Exhibit 1, email the contact provided on the cover page of this document.

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

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

Provide rate schedule for the high-level deliverables defined RFP Section 1.1.4 Scope of Work.

The Respondent 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.

Year 4 Cost is the cost for travel to the Institution/location identified for Year 4.

Year 5 Cost is the cost for travel to the Institution/location identified for Year 5.

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

Exhibit 1 (Table 3) – Respondents will use this attachment to record all costs associated with this section. For a copy of the excel version of Exhibit 1, email the contact provided on the cover page of this document.

#	Travel Cost	Year 1 Cost	Year 2 Cost	Year 3 Cost	Year 4 Cost	Year 5 Cost	Optional Renewal (Year 1)	Optional Renewal (Year 2)	Optional Renewal (Year 3)
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								
	-								
	-								

Appendix D – Contract for Services

UNIVERSITY OF MAINE SYSTEM
MASTER AGREEMENT

This Contract for Services Master Agreement ("Agreement" or "Master 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 – Insurance Requirements

Rider C – University of Maine System Standards for Safeguarding Information

Rider D – Services Engagement Form

Contract Amendments as required

Request for Proposal #2020-017 Issue Date December 3, 2019 Titled PCI Data Security Penetration Testing
Contractor's Bid in Response to Request for Proposal #2020-017 Proposal Submission Date December 13, 2019 Titled 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 **Rider 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 D**. 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 January 1, 2020 and shall terminate on December 31, 2025, unless terminated earlier as provided in this Contract with option for **three (3) one (1) year or one (1) three (3) year renewals** upon the parities' mutual written 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. "**Additional Services**" The University will have the option to purchase additional services under this Agreement.

      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 D**.

4. **Termination:** The **Agreement or a Services Engagement (Rider D)** 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:** University of Maine System, Chief Security Officer shall be the University's authorized representative in all matters pertaining to the administration of the terms and conditions of this Contract.

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. This Contract is the entire agreement between the University (including University's employees and other End Users) and Contractor. In the event that Contractor enters into terms of use agreements or other agreements, policies or understandings, whether on Contractor's purchase order, website, electronic, click-through, verbal or in writing, with University's employees or other End Users, such agreements shall be null, void and without effect, and the terms of this Contract shall apply. University will not be bound to any other terms and conditions set forth in any documents, agreements or policies posted on Contractor's website unless such terms and conditions are set forth in this Contract. Contractor may not unilaterally change any term or condition of this Contract.

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
Robinson Hall
46 University Drive
Augusta, ME 04330

Attn: **Contract Administration**

To Contractor:

<<NSTRUCTIONS – Respondent to supply information noted below for submission >>
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:

    University of Maine System
    Accounts Payable
    PO Box 533
    Bangor, ME 04402

    Phone: 207-581-2692
    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** – Insurance Requirements
    E. **Rider C** – University of Maine System Standards for Safeguarding Information
    F. **Rider D** – Services Engagement Form
    G. **Contract Amendments** as required
    H. **Request for Proposal** #2020-017 Issue Date December 3, 2019 Titled PCI Data Security Penetration Testing
    I. **Contractor's Bid in Response to Request for Proposal #**2020-017 Proposal Submission Date December 13, 2019 Titled 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.

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 if it is not approved, valid or effective until such written approval is granted."

Chief Financial Officer approval is required of any University of Maine System agreement of $50,000 or more, and it is not approved, valid or effective until such written approval is granted.

Chief Business Officer approval is required of any campus specific agreement of $50,000 or more, and it is not approved, valid or effective until such written approval is granted.

BY: _____

Title: _____

Chief Procurement Officer or designee

Date: _____

BY: _____

Title: _____

Chief Financial/Business 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 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:

Penetration testing will include internal and external testing on network devices residing at University of Maine System Institutions. Bidders may choose to travel to campus locations at their discretion to provide their most effective penetration testing services.

Level I Penetration Testing Deliverables - Penetration testing for each Institution will require testing for the payment devices identified. Penetration testing will meet the minimum requirements of **PCI DSS 3.2.1 (section 11.3),** as well as, meeting the following University requirements:

2. Penetration testing from both inside and outside the network.
3. Testing to validate any segmentation and scope-reduction controls.
4. Verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from in-scope systems.
5. Specify remediation.
6. 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.
    b. Application-layer penetration tests (where applicable) that include the vulnerabilities noted in the **PCI DSS 3.2.1 Requirements (Sections 6.5.1 - 6.5.10).** 6.5.1 - Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws.
    c. 6.5.2 - Buffer overflows
    d. 6.5.3 - Insecure cryptographic storage
    e. 6.5.4 - Insecure communications
    f. 6.5.5 - Improper error handling
8. Provide a Level I findings report with identified remediations.

Level II Penetration Testing Deliverables - Additionally there may be Institutions which require targeted penetration testing for a web application or system that supports the payment environment. Such requirements will include testing of vulnerabilities described in current OWASP, or similar, security guidance and those noted in the **PCI DSS 3.2.1 Requirements (Sections 6.5.7 - 6.5.10**).

2. 6.5.7 - Cross-site scripting (XSS)
3. 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).
4. 6.5.9 - Cross-site request forgery (CSRF)
5. 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.

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

Level III - UMS Institutions may need additional penetration testing services to confirm alignment with other security or compliance frameworks (e.g. NIST-800 171). The scope (e.g. numbers of systems and networks) and complexity of such tests will be determined by consultation with the system owner for the specific compliance need. Offerings should include testing at various levels, to include at a minimum:

- 1. Confirmation of proper network segmentation
- 2. Identification and validation of vulnerabilities of network facing services
- 3. Leveraging detected vulnerabilities for lateral movement within sets of identified systems
- 4. Application-specific testing, to include Web Application testing, to identify at a minimum OWASP Top 10 vulnerabilities.

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 jointly develop 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.

An estimate of Year 1 scheduled activities is detailed in the table directly below and will form the deliverables required for the first Service Engagement form. Counts and locations are subject to change due to ongoing updates that could affect the need to pentest specific cardholder environments. 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	75	Level I	January 15, 2020
2	University of Maine at Farmington	Farmington. Maine	10	Level I	January 15, 2020
3	University of Southern Maine	Portland, Maine	10	Level I	January 15, 2020
4	University of Maine at Augusta	Augusta. Maine	10	Level I	January 15, 2020
5	University of Maine at Fort Kent	Fort Kent, Maine	3	Level I	January 15, 2020
6	University of Maine at Machias	Machias, Maine	3	Level I	January 15, 2020
7	University of Maine at Presque Isle	Presque Isle, Maine	2	Level I	January 15, 2020

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.

PRICING: Refer to RIDER A-1. Pricing will be valid for the term of the Agreement.

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:** If the solution, services or deliverables include any Information or Communication Technology (ICT) containing a human-interface, such as an end-user software component, web pages or site, video or audio playback, file upload system, mobile device components, control panel, reports, documents, keypad, etc., the Contractor hereby warrants that the products and/or services to be provided under this agreement comply with the W3C's Web Content Accessibility Guidelines (WCAG) 2.0 Level AA and the Web Accessibility Initiative Accessible Rich Internet Applications Suite (WAI-ARIA) 1.1 for web content

   The Contractor agrees to promptly respond to and resolve any complaint regarding accessibility of its products or services which is brought to its attention and Contractor further agrees to indemnify and hold harmless the University of Maine System 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 Contractor's products or services covered by this agreement to ensure compliance with the above standards.

   Complaints, or testing, that results in findings of non-compliance, that are not corrected within 30 days of being reported to the Contractor in writing, shall constitute a breach of this agreement and shall be grounds for termination of this agreement and a pro-rated refund of fees paid by the University.

6. **Standards for Safeguarding Information:** The Contractor is expected to comply with these standards as outlined in ***Rider 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.

RIDER A-1
PRICING

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

RIDER B
INSURANCE REQUIREMENTS

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, including Product's and Completed Operations (Written on an Occurrence-based form) (Bodily Injury and Property Damage)	$1,000,000 per occurrence or more
2	Vehicle Liability (Including Hired & Non-Owned) (Bodily Injury and Property Damage)	$1,000,000 per occurrence or more
3	Workers Compensation (In Compliance with Maine and Federal Law)	Required for all personnel
4	Professional Liability Insurance (Agents, Consultants, Brokers, Lawyers, Financial, Engineers, or Medical Services)	$1,000,000 per occurrence or more
5	Cyber Liability Insurance (If PII or PHI is stored on systems managed by the provider, the coverage is mandatory.)	$1,000,000 per occurrence or more

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:

University of Maine System
Risk Manager
Robinson Hall
46 University Drive
Augusta, Maine 04330

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 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
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 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:

PRICE:

SIGNATURES:

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

Chief Information Officer approval is required of any University of Maine System information technology service engagements.

BY: _____

Title: _____

Chief Information Officer or designee Date: _____

Appendix E – Evaluation Question(s) – Master Agreement

This portion of the RFP contains special terms and conditions which will govern the resulting agreement, many of which are stated in Section 1.2 of the RFP, with more detail in Appendix D. Please indicate your acceptance for each special term by checking the "Agreed" box and initialing.

Should you take exception to any of these special terms and conditions you are required to note your exception directly below each of the respective terms in question. It should be noted that any exceptions may result in the disqualification of your proposal, lack of providing the required response or indicating terms will be negotiated post award will result in a zero (0) score for the Master Agreement evaluation criteria in Section 2.1.1.

1.1 Terms and Conditions of Agreement

As a result, of this RFP process, it is our expectation that an Agreement will be established between University and one or more of the Contractors. The Agreement will incorporate the relevant terms and conditions of this RFP and Contractor's proposal (scope of work, pricing, service level agreement, warranty, implementation plan).

Upon award each successful Agreement or will sign a Master Agreement (Appendix D) with the University to sell goods and/or services. The Agreement will incorporate all the terms and conditions, pricing, specifications, and requirements of the RFP.

No representation is made that any quantities will be purchased or that services will be utilized.

☐ **Agreed** _____

Initial

1.2 Agree to term other than what is specified or automatic renewals for term(s) greater than month-to-month.

Appendix D - 2. Term
The Agreement term will be for five (5) years with the option of four (4) one-year renewals. Exercise of any renewal option will require parities' mutual written agreement.

☐ **Agreed** _____

Initial

1.3 Agree to termination language other than what is provided in Appendix D, Section 4, 5, and 6.

Appendix D - 4. Termination: The **Agreement or a Services Engagement (Rider D)** 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 affected by delivery to the Agreement or 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 Agreement or shall not be reimbursed for any costs incurred after the effective date of termination.

☐ **Agreed** _____

Initial

Appendix D - 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 Agreement or for all services performed to the effective date of termination subject to offset of sums owed by the Agreement or to the University.

☐ **Agreed** _____

Initial

Appendix D - 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.

☐ **Agreed** _____

Initial

1.4 Permit an entity to change unilaterally any term or condition once the Agreement is signed;

Appendix D - 8. Modification:
This Agreement may be modified or amended only in a writing signed by both parties.

☐ **Agreed** _____

Initial

1.5 Apply the law of a state other than Maine;

Appendix D - 10. Applicable Law:
This Agreement shall be governed and interpreted according to the laws of the State of Maine

☐ **Agreed** _____

Initial

1.6 Provide any defense, hold harmless or indemnity;

Appendix D - 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

☐ **Agreed** _____

Initial

1.7 Waive any statutory or constitutional immunity;

☐ **Agreed** _____
Initial

1.8 Pay attorneys' fees, costs, expenses or liquidated damages;

☐ **Agreed** _____
Initial

1.9 Accept any references to terms and conditions, privacy policies or any other websites, documents or conditions referenced outside of the Agreement .

Appendix D - 17. Entire Agreement:
This Agreement 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. This Agreement is the entire agreement between the University (including University's employees and other End Users) and Agreement or. In the event that Agreement or enters into terms of use agreements or other agreements, policies or understandings, whether on Contractor's purchase order, website, electronic, click-through, verbal or in writing, with University's employees or other End Users, such agreements shall be null, void and without effect, and the terms of this Agreement shall apply. University will not be bound to any other terms and conditions set forth in any documents, agreements or policies posted on Contractor's website unless such terms and conditions are set forth in this Agreement. Agreement or may not unilaterally change any term or condition of this Agreement.

☐ **Agreed** _____
Initial

1.10 Promise confidentiality in a manner contrary to Maine's Freedom of Access Act;

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

☐ **Agreed** _____
Initial

1.11 Procure types or amounts of insurance beyond those UMS already maintains or waive any rights of subrogation.

☐ **Agreed** _____
Initial

1.12 Add any entity as an additional insured to UMS policies of insurance.

☐ **Agreed** _____
Initial

Appendix F – Organization Reference Form

Respondent's Organization Name: _____

INSTRUCTIONS: Provide a minimum of three (3) current professional references who may be contacted for verification of the Respondent's professional qualifications to meet the requirements set forth herein. We strongly prefer references from higher education institutions similar in size and requirements to the University of Maine System, including those with multi-campus integrated solutions.

We request that the references include one long-standing customer (minimum of 3 year engagement) and one new customer (one who has been engaged with Respondent for less than one year).

REFERENCE #1	
Institution/Company Name	
Contact Name	
Contact Title	
Contact Phone Number	
Contact eMail Address	
Relationship Length	

REFERENCE #2	
Institution/Company Name	
Contact Name	
Contact Title	
Contact Phone Number	
Contact eMail Address	
Relationship Length	

REFERENCE #3	
Institution/Company Name	
Contact Name	
Contact Title	
Contact Phone Number	
Contact eMail Address	
Relationship Length	

REFERENCE #4	
Institution/Company Name	
Contact Name	
Contact Title	
Contact Phone Number	
Contact eMail Address	
Relationship Length	

Appendix G – Evaluation Question(s) - Organization, Qualifications and Experience

Respondent's Organization Name: _____

INSTRUCTIONS: Respondents shall ensure that all information required herein is submitted with the response. 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 response or rescission of an award. Respondents are encouraged to provide any additional information describing operational abilities.

Evaluation Question(s)

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?

2. If subcontractors are to be used, provide a list that specifies the name, address, phone number, contact person, and a brief description of the subcontractors' organizational capacity and qualifications.

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

4. Describe your experience offering a solution for the business requirements identified in this document within higher education. Provide a client list that includes any and all higher education clients.

5. 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 Respondent must demonstrate that they are a recognized leader in the services and/or products covered in this document.

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

Appendix H – Evaluation Question(s) – Information Technology

Respondent's Organization Name: _____

All responses to the questions will reflect what is offered as part of the Respondent's proposed solution. Respondents **MUST** indicate if the product or service requires modification, additional products or services, or if any other accommodation would be necessary to meet a requirement.

Evaluation Question(s) - General Technical

1. Describe your process for performing PCI DSS Penetration Testing as to meet the minimum requirements set forth by **PCI DSS 3.2.1.**

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

.

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

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

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

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

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

8. Describe your availability to being able to complete the penetration tests within the timetable set in section **1.1.4 Specifications/Scope of Work**. including any ability to perform some or all of the work remotely Additionally describe your expected lead time for future engagements.

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.

10. Provide confirmation that you can meet the complete date for the deliverables noted in **1.1.4 Specifications/Scope of Work, Table 1**.