University of Maine System
PCI Data Security Penetration Testing - RFP # 36-15
ADDENDUM #1 – ANSWERS TO VENDOR QUESTIONS

QUESTIONS

1. Can you give me a break down of how many active internal and external IPs you want in scope?
   ANSWER:

   The numbers I am quoting are approximate. If your company bills by IP address than you need to structure the cost appropriately so we understand the per cost for an external and internal IP testing.

   - External ~ 40 IP's
   - Internal ~ 80 IP's

2. For each of the 4 institutions requiring testing, please confirm the number of active *external* hosts?
   ANSWER:

   The numbers are ***approximate***. The numbers below represent the number of external IP's.

   - University of Maine - Orono 20 External IP's
   - University of Maine at Farmington 10 External IP's
   - University of Southern Maine 5 External IP's
   - University of Maine at Augusta 5 External IP's

3. For each of the 4 institutions requiring testing, please confirm the size of the *internal* cardholder data environment as far as # of systems in scope.
   ANSWER:

   The numbers are ***approximate***. The numbers below represent the number of internal IP's.

   - University of Maine - Orono 40 Internal IP's
   - University of Maine at Farmington 7 Internal IP's
   - University of Southern Maine 25 Internal IP's
   - University of Maine at Augusta 15 Internal IP's

4. Please confirm the total number of public-facing websites requiring testing. In order to estimate the time and effort required for web application testing, we need to determine the size/complexity of the website (# of dynamic pages, forms/inputs, overall functional attributes). Please provide a brief description of the website (purpose, user base, data characteristics) along with what functionality will be available with and without authentication.

   ANSWER:

We have one public-facing website requiring testing. The url for the site is: https://tickets.collinscenterforthearts.org. The user base is the general public and the purpose of the site is to provide customers the ability to purchase theater tickets for events held at the University of Maine campus.

The data characteristics include a search feature, which allows customers to search for specific shows and performance dates. Account creation is available as is the ability to pay for their purchase from this site. As far as authentication, customers are required to create an account to complete a ticket purchase. If a customer forgoes the creation of an account all they can do is search the site.

5. Are the additional 4 locations identified in Table 3 (Bangor, Machias, Presque Isle, Fort Kent) 'Travel Expenses' relevant and in scope for the purposes of this RFP response?
ANSWER:

The four locations listed in the aforementioned are not part of this first engagement, we are looking for 'Travel Expenses' pricing only for potential future engagements at those locations.

6. Are you looking to have a PCI Gap Assessment, Report on Compliance, or Both?
ANSWER:

We are not looking for a PCI Gap Assessment (where we are looking for a vendor to evaluate the University's readiness to pass a PCI On-Site Assessment) we are looking for a vendor to provide penetration testing on specific CDE's in accordance with the PCI DSS SAQ Requirements and define areas where the University does not comply with the Payment Card Industry Data Security Standard (PCI DSS), and outlines areas requiring remediation.

7. Provide a quick description to the business process(s) this assessment will focus on. Briefly describe how cardholder data is stored, transmitted, and processed during this process(s).
ANSWER:

We do not store any cardholder data. We have 13 merchants (8 SAQ C's and 5 SAQ D's) in scope for this first engagement. They are housed in 7 payment environments at 4 campus locations. (UM has 3, USM has 2, UMF has 1, and UMA has 1.)

8. Are there any service providers in-scope for this assessment. If so, please list the name and what the provider is contractually obligated to do. Service providers could include but is not limited to:

- 3rd party monitoring vendors
- Web hosting providers
- Cloud providers
- etc

ANSWER:

The University has secured the services of **Solutionary Managed Security Services**. We utilize ActiveGuard (Security and Compliance Platform) which collects and correlates vast amounts of data from University devices capable of producing a log file such as endpoints, firewalls, IDS, and network devices. ActiveGuard enriches gathered security data with a variety of contextual information such as vulnerabilities, assets, GeoIP, malicious hosts, privileged and non-privileged users to detect threats and increase accuracy.to provide analysis, validation and response for security threats. The advanced analytics in ActiveGuard, in combination with threat intelligence from the help to detect advanced threats and zero-day attacks.

9. Approximately how many systems will be included in-scope of this assessment:

ANSWER:

Each merchant environment has 1-2 servers. Therefore, 90+ percent of all non-network nodes are clients (workstations or laptops). No wireless is in scope at this time.

1) Laptop/Desktop
2) Network devices (routers, switches, firewalls)

Network devices:	FW	Routers	Switches
UM	1	1	20
USM	2	1	15
UMA	1	1	5
UMF	0	1	10

3) Servers (Windows 2003, 2008, 2012, etc)

Each merchant environment has 1 - 2 servers, it is not known at this point what platform is running the servers.

10 Please list the addresses of the facilities that will be in-scope for this assessment (i.e. Corporate headquarters, datacenter, etc)

ANSWER:

University of Maine - The University of Maine 119 College Avenue, Orono, Maine 04469
University of Maine at Farmington - 111 South Street, Farmington, ME 04938
University of Maine at Augusta - 46 University Drive, Augusta, ME 04330
University of Southern Maine - 96 Falmouth Street, Portland, ME 04103

11 Has a dedicated network segmented been carved out for the Card Data Environment (CDE)?

ANSWER:

We have dedicated network segments for each of our Card Data Environments.

12 List all applications that store, transmit, and process cardholder data
ANSWER:

We do not store any cardholder data. Systems vary from merchant to merchant, with that being said, we do use TouchNet and Sequoia as third party processors.

13 In approximately how many areas is cardholder data stored? Is the data encrypted?
ANSWER:

We do not store cardholder data in any Card Data Environment. All card data that leaves our internal secure network is encrypted when transmitted or processed.