**RFP05222023 – Payment Card Industry Data Security Standards Compliance Services**

**Q&A #2**

* How many of each SAQ type(s) do you have?
  + *This information will be provided during the pre-bid call.*
* Do you want QSA sign off on the SAQ's or just help and consulting?
  + *As stated in the RFP page 3 section 1 point one, “This assessment may include, but is not limited to: penetration testing, internal/external scans, SAQ assistance.”*
* Are all merchants located on 1 campus?
  + *No*
  + If not, how many locations are there?
    - *One Merchant is in Hot Springs, Arkansas*
  + How far away is each location from the main campus?
    - *Hot Springs is 200 miles from the UAF campus.*
* Do you have a deadline for validating your PCI compliance?
* *Our yearly deadlines are as follows: UAF February 1, Arkansas Alumni Association (AAA) February 1, University of Arkansas Foundation April 1*
* Do you have centrally-controlled policies and procedures that would facilitate sampling of SAQ B, SAQ B-IP, and/or SAQ P2PE campus merchants.
  + *Policies can be located at* [*https://vcfa.uark.edu/fayetteville-policies-procedures*](https://vcfa.uark.edu/fayetteville-policies-procedures) *Sampling can happen at the university’s discretion.*
* According to the RFP, *“As level-3 merchant these merchants perform their own assessments using internal questionnaires, device inventory, and access control lists. Merchant transactions run the gamut including card-present, card-not-present, and e-commerce with various point-of-sale systems resulting in various Self-Assessment Questionnaire (SAQ) levels that result in an SAQ-D roll-up to the bank.”*
  + How many acquirers (i.e., banks) do you provide reports to?
    - *Reports are provided to three acquirers.*
  + Approximately how many point-of-sales systems do you have? Are all your point-of-sales systems from the same vendor?
    - *This information will be provided during the pre-bid call.*
  + Is the e-commerce website(s) owned/managed by the University including the payment page or is it outsourced?
    - *Payment pages are hosted payment sites.*
  + For the various SAQs that are performed by each merchant, could you please provide a listing of the SAQ levels?
    - *This information will be provided during the pre-bid call.*
  + Are you utilizing any Cloud Services?
    - *Yes, cloud services are utilized.*
  + How many separate physical locations are processing (card present) credit cards?
    - *All merchants are physically located on the Fayetteville campus with the exception of one location in Hot Springs that utilizes four unique MIDs (two UAF and two UA Foundation).*
* According to the RFP, *“The University of Arkansas is also responsible for validating the PCI compliance for the Arkansas Alumni Association (AAA) and UAF related activity of the University of Arkansas Foundation. AAA is staffed by University employees and has one credit card merchant account used for online, in person and mail order/telephone transactions. Select University employees accept and process transactions on behalf of the Foundation across four credit card merchant accounts.”*
  + Do the AAA compliance efforts also roll into the SAQ D or is it a separate attestation?
    - *AAA completes and submits a separate SAQ-D.*
  + If the AAA is reported separately, is the reporting period (compliance date) the same as you other reporting date(s)?
    - *AAA reporting period is February 1.*
  + For the mail order transactions, are these processed by the University internally or are you utilizing a lockbox service?
    - *AAA mail order transactions are processed by a lockbox service.*
* General
  + Is there any flexibility within the agreement (e.g., the indemnification section) in the event our in-house counsel requests a minor change?
    - *It is unlikely that the indemnification section can have minor changes. Any desired changes need to be submitted in advance for University general counsel to review.*
  + Are there any requirements to perform the work onsite or is a hybrid approach (e.g., site visits by members of our Arkansas team combined with remote status meetings) acceptable?
    - *A hybrid approach is acceptable for this project.*

For **Penetration Testing** (as it pertains to the card holder environment)

External network:

* List of sites and purpose of site (data center, remote office, etc.) containing an internet facing network infrastructure to be tested
  + *This list will vary from year to year and will be provided to the respondent for scoping at the time of penetration testing.*
* Quantity of IP ranges at each site, the quantity of IP addresses available within each range, and estimates of how many live IP addresses would be expected to respond within each IP range
  + *This list will vary from year to year and will be provided to the respondent for scoping at the time of penetration testing.*

Internal network:

* List of sites and purpose (data center, remote office, etc.) containing a private network infrastructure to be tested
  + *This list will vary from year to year and will be provided to the respondent for scoping at the time of penetration testing. Penetration testing scope will come after the assessment and evaluation of the current framework.*
* Quantity of IP ranges at each site, the purposes of those ranges such as “servers” or “network management”, and identifying the quantity of hosts of each type
  + *This list will vary from year to year and will be provided to the respondent for scoping at the time of penetration testing. Penetration testing scope will come after the assessment and evaluation of the current framework.*

Segmentation testing (if utilized):

* Number of PCI related networks requiring segmentation testing
  + *16-50 subnets for segmentation testing This list will vary from year to year and will be provided to the respondent for scoping at the time of penetration testing. Penetration testing scope will come after the assessment and evaluation of the current framework.*

For **Vulnerability Scanning** (as it pertains to the card holder environment)

* Number of external facing IPs to be scanned
  + *25-50 External facing IP Addresses to be scanned. This list will vary from year to year and will be provided to the respondent for scoping at the time of penetration testing. Penetration testing scope will come after the assessment and evaluation of the current framework.*
* Number of internal assets to be scanned
  + *This list will vary from year to year and will be provided to the respondent for scoping at the time of penetration testing. Penetration testing scope will come after the assessment and evaluation of the current framework.*

**Payment Card Industry Data Security Standards (PCI DSS) Compliance Services**

Questions

* Is there an incumbent who is currently providing these services?
  + *No*
    - If yes, is the incumbent performing to the satisfaction of the University Of Arkansas (UA)? *N/A*
    - Is the incumbent eligible to bid on this contract? *N/A*
    - Is there a reason for considering the replacement of the incumbent? *N/A*
* Is this the first time you will contract a vendor(s) for the services in question?
  + *Yes*
    - If not, would a copy of the final contract, amount, and hourly rates of the previous successful vendor(s) be available? *N/A*
* Can offshore personnel (outside the United States) work on this project?
  + *While there is no current prohibition for offshore work, it would need to be disclosed up front along with the locations from which individuals would be working.*
* Is there a budget for this project? Are you able to provide the budget estimate?
  + *The University will not disclose the project budget or estimate at this time.*
* Are the services expected to be performed onsite? Remotely? Both? If so, please describe the frequency of onsite visits.
* *Services may be completed remotely or on a hybrid basis with an expectation of at least one on-site visit per year.*
* Is there a preference for a company with DVBE, SB, MVE etc. certifications?
  + *We need to confirm the answer to this question with our Procurement Team. A response will be provided during the pre-bid call.*
* Is there a sample agreement to review?
  + *If you're referring to a sample agreement between your entity and UAF, please refer to the Terms and Conditions found throughout the subject RFP. We may use a contract generated/provided by the successful bidder; however, it will need to include the Terms and Conditions as provided for in the body of the RFP.*
* Did the entity name receive 3rd party assistance in preparing this RFP?
  + *Yes*
* What are the most important expectations you have for a compliance/security partner?
  + *Please see page 3 starting at “UA expects to achieve the following”.*
* What are your top requirements for the vendor you choose, which will set them apart from other bidders?
  + *The university seeks a bidder that will be collaborative, flexible, and listen to the specific needs and objectives of UA staff. The selected bidder will have higher education experience and be able to provide thought leadership and industry best practices to our team.*
* How is success defined for this project?
  + *Success will be defined by having the selected bidder complete the technical work in scope for this project along with developing an ongoing, dynamic, and collaborative relationship with university stakeholders that leads to an overall increase in the effectiveness and efficiency of the university's payment card compliance program.*
* Who are the key stakeholders for this project?
  + *The key stakeholders for this project are the University of Arkansas Finance and Administration Compliance team, Cash Management team, and the Information Security team.*
* Are wet signatures required, or will digital signatures suffice?
  + *Digital signatures are acceptable.*
* Please clarify the frequency of the penetration testing and vulnerability scanning.
  + Monthly? Quarterly? Annually?
* *Penetration testing will be done annually and on an ad hoc basis.*
* **Please provide the following for the University’s Cardholder Data Environment**
  + Total count of External IPs? *Penetration testing scope will come after the assessment and evaluation of the current framework.*
  + Total number of internal IP addresses to be tested (if providing an IP range, please indicate the estimated number of live IPs) *Penetration testing scope will come after the assessment and evaluation of the current framework.*
  + How many Desktops/Laptops? *N/A*
  + How Many Servers (both virtual and physical)? *N/A*
    - How many are on-prem and in the cloud? *N/A*
  + How many firewalls are in place at UA? *N/A*
  + How many routers/switches/access points are in the environment? *N/A*
  + How many printers and scanners are in the environment? *N/A*
  + How many surveillance cameras does UA have in scope? *N/A*
* How many VOIP devices are in scope? *N/A*
* Are there any web applications in scope for this project? *Penetration testing scope will come after the assessment and evaluation of the current framework.*
  + If so, how many are publicly available?
  + Are there any web applications that will require code review? (i.e., custom applications built and owned solely by UA)
    - *There are no web applications built and owned solely by the UA included in this RFP.*
* How many wifi networks do you have? *2 Main wifi networks and a dozen specialty networks*
  + Do you have a dedicated guest network?
    - *Yes, we have a dedicated guest Wi-Fi network.*
* How many locations/sites would be part of the scope?
* Are all internal target systems and subnets accessible from a single location, or will travel to other facilities be necessary for the internal testing?
* Is there a specific type of testing being requested by UA? (white/gray/black box).
  + If not, will it be the Consultant or the decision of UA to decide?
    - *The type(s) of testing to be conducted will be a collaborative decision.*
* **Please provide the following for the Finance and Administration systems**
* Total count of External IPs? *Penetration testing scope will come after the assessment and evaluation of the current framework.*
* Total number of internal IP addresses to be tested (if providing an IP range, please indicate the estimated number of live IPs)
  + How many Desktops/Laptops? *N/A*
  + How Many Servers (both virtual and physical)? *N/A*
    - How many are on-prem and in the cloud? *N/A*
  + How many firewalls are in place at UA? *N/A*
  + How many routers/switches/access points are in the environment? *N/A*
  + How many printers and scanners are in the environment? *N/A*
  + How many surveillance cameras does UA have in scope? *N/A*
  + How many VOIP devices are in scope? *N/A*
* Are there any web applications in scope for this project? *Penetration testing scope will come after the assessment and evaluation of the current framework.*
  + If so, how many are publicly available?
  + Are there any web applications that will require code review? (i.e., custom applications built and owned solely by UA)
    - *There are no web applications built and owned solely by the UA included in this RFP.*
* How many wifi networks do you have? *Two main Wi-Fi networks and a dozen specialty networks.*
  + Do you have a dedicated guest network?
    - *Yes, we have a dedicated guest Wi-Fi network.*
* How many locations/sites would be part of the scope?
  + *Penetration testing scope will come after the assessment and evaluation of the current framework.*
* Are all internal target systems and subnets accessible from a single location, or will travel to other facilities be necessary for the internal testing?
  + *Penetration testing scope will come after the assessment and evaluation of the current framework.*
* Is there a specific type of testing being requested by UA? (white/gray/black box).
  + If not, will it be the Consultant or the decision of UA to decide?
    - *This will be a collaborative decision on what type of testing is conducted.*

* Does UA use endpoint detection (EDR/XDR) software? *This information will be provided to the selected bidder upon completion of the contract and start of the project.*
* What security products do you already have (e.g., firewall, intrusion detection, encryption)? *This information will be provided to the selected bidder upon completion of the contract and start of the project.*
* How many financial systems will need additional penetration testing and vulnerability scanning services? *This information will be provided to the selected bidder upon completion of the contract and start of the project.*
* Please provide the digital infrastructure for the additional financial systems requiring penetration testing. *This information will be provided to the selected bidder upon completion of the contract and start of the project.*
* Will any of the policies need to be drafted from scratch, or do existing policies solely require updates/development?
  + *Policies exit and can be located at:* [*https://vcfa.uark.edu/fayetteville-policies-procedures*](https://vcfa.uark.edu/fayetteville-policies-procedures)
* Will the Incident Response Plan need to be drafted from scratch or solely require updates/review?
  + *The Incident response plan exists and will need to be reviewed/updated.*
* Please provide a list of UA’s current information security policies, if allowed.
  + Alternatively, please give the total count of existing information security policies if you cannot provide a list.
    - *Policies can be located at* [*https://vcfa.uark.edu/fayetteville-policies-procedures*](https://vcfa.uark.edu/fayetteville-policies-procedures)
* Which SAQ type is the UA attesting to?
  + SAQ-A, SAQ-D, SAQ-C-VT…etc.
  + *This information will be provided during the pre-bid call.*
* What assets require testing for the technology assessment?