SEDGWICK COUNTY, KANSAS
DIVISION OF FINANCE
PURCHASING DEPARTMENT
525 N. Main, Suite 823 ~ Wichita, KS 67203
Phone: 316 660-7255 Fax: 316 383-7055

www.sedgwickcounty.org/purchasing

REQUEST FOR PROPOSAL
#13-0020
PCI SCANNING SERVICES

ADDENDUM #2

April 3, 2013

The following information is in regard to **RFP 13-0020**

Questions are in bold, *answers are in italics.*

1. **General Questions**
   a. **Is the County willing to entertain a phased approach? For example,**
   Phase 1 – Includes Executive Level Briefing, Isolated Network Design, and Scope Reduction/Remediation Planning
   Phase 2 – Includes Gap Analysis, Penetration Testing, and Vulnerability Scanning
   Successful scope reduction and network design strategies should reduce the level of effort for activities Phase 2 (in-scope system inventory would be lower than current). Quoting Phase 2 activities, without understanding the benefits resulting from Phase 1 should, in theory, be artificially higher.
   Yes

   b. **Per question 1, would the county like to see a la carte pricing for the existing environment ("as-is"), with the expectation that scope reduction activities impact the level of effort for a Gap Assessment, Penetration Testing, and Vulnerability scanning?**
   Yes

2. **PCI Gap Analysis**
   a. **Are all applications are commercial off the shelf ("COTS") applications, or is there a mix of COTS and internally developed applications**
   Mix

   b. **Do Perimeter (Internet Facing) Firewalls exist?**
   Yes

   c. **Does Internal Segmentation (via firewalls or router/switch based ACLs) exist?**

Yes

d. Does your organization have centralized corporate security policies?
No

e. Is cardholder data stored anywhere in clear text?
Not to the best of our knowledge.

f. Are formal key management processes in place for all applications and databases that store, process or transmit cardholder data?
Please define key management via an example.

g. Has logging been enabled for all system components (applications, firewalls, routers, servers, databases, etc.) that store, process or transmit cardholder data?
No

h. Are all logs stored on centralized logging management system?
No

i. Has the organization been conducting quarterly vulnerability scans across the internal and perimeter (Internet facing) networks?
Yes

j. Has the organization conducted penetration testing for internal and perimeter (Internet facing) networks over the past year?
No

k. Please complete the following inventory data points as applicable
All devices are point to point on VLANs from County to Bank, do not knowingly store data. This is information we are hoping to obtain through the scope reduction process.

3. PCI Penetration Testing

a. How many external IP addresses will we be searching through to identify live hosts / targets (ex "2 /24 networks, 3 /22 networks)?
There are only 2 hosts in PCI scope.

b. How many internal IP addresses will we be searching through to identify live hosts / targets (ex "2 /24 networks, 3 /22 networks)?
There are 14-Class C24 networks.

c. How many external live hosts will we be performing penetration testing services against?
Unknown, penetration testing has never been done.

d. **How many internal live hosts will we be performing penetration testing services against?**
Unknown, penetration testing has never been done.

e. **Will testing be limited to specific windows? If Yes, please specify windows and other details.**
Unknown, penetration testing has never been done.

f. **Can Bidder perform internal testing using a remote internal laptop? This solution has the potential to reduce travel costs and improve scheduling time to complete your project.**
Possibly, this topic requires more discussion and vendor must be vetted.

g. **Will you require Bidder to conduct retesting upon completion of the project to demonstrate that identified external vulnerabilities were appropriately remediated? Note: This only applies to external testing.**
Yes

h. **Is quarterly internal vulnerability scanning in-scope for this response?**
Yes

4. **Approved Scanning Vendor (ASV) or External Vulnerability Scanning.**
   a. **What public IP space does your company have?**
   205.172.12.0/24; 205.172.13.0/24; 205.172.14.0/24 and 205.175.15.0/24

   b. **Number of "live" external/internet facing IPs addresses within your public IP space?**
   Two (2) in PCI Scope.

   c. **What publicly accessible domain names does your organization own?**
   Only one (1) in scope through sedgwickcounty.org (perhaps others-part of scope reduction process)

   d. **How many systems are in your DMZ? (a DMZ is the protected network for your web accessible systems)**
   Only two (2) in PCI scope, but many others outside scope.

   e. **Who is your Acquiring Bank, or entity that oversees cardholder processes?**
   The Merchant Service Provider is Point and Pay who uses Global Pay to process. Exploration Place uses Commerce Bank, the Zoo is unknown at this time.

5. **Application Assessment**
   a. **Is PCI requirement 6.6 in-scope for this response:**

   6.6 For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods:

i. **Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes**

ii. **installing a web-application firewall in front of public-facing web applications**

Yes

b. If Web Applications are in-scope per requirement 6.6, please provide the following for each:

i. What type of application will Bidder be assessing?

1. Browser-based HTML

2. Browser-based Rich Media

Browser-based HTML

Vendors are responsible for checking the web site and **acknowledging any addendums on the proposal response form**.

Digitally signed by Kimberly Evans
DN: cn=Kimberly Evans, o=Sedgwick County, ou=Purchasing, email=kjevans@sedgwick.gov, c=US
Date: 2013.04.03 11:04:28 -05'00'

_____

Kimberly Evans
Purchasing Agent