City of Wheaton
303 W. Wesley Street
Wheaton, IL 60187-0727
630-260-2000
City of Wheaton, Illinois
www.wheaton.il.us

CYBERSECURITY CONSULTING SERVICES

Request for Proposal Amendment #6

The following changes / clarifications / additions have been added to the Request for Proposal project specifications and plans:

1. **QUESTION:** Scope 3: Jan 2017 (every 6 months) External Penetration Test: Is the City of Wheaton interested in a single pen test with included follow-up scans to verify remediation was successful? Or two complete external pen tests per year?
   ANSWER: We are seeking two external penetration tests every year.

2. **QUESTION:** Scope 5: Mar 2017 (every 6 months) PCI Cardholder Data Environment (CDE) Penetration Test: Is the City of Wheaton interested in a single pen test with included follow-up scans to verify remediation was successful? Or two complete external pen tests per year?
   ANSWER: The PCI Cardholder Data Environment (CDE) Penetration Test is an internal penetration test. This test is to ensure that a host on our internal network cannot access or compromise the hosts in the CDE. We are seeking two internal CDE penetration tests every year.

3. **QUESTION:** Scope 9: On Demand Training Advisory Services: Can you provide more detail around the types of training you might be interested in? Security Awareness Training for end-users? Incident Response Planning guidance?
   ANSWER: The question was answered in Amendment #3 question 6.

4. **QUESTION:** Scope 14: Optional Annual Security Log Monitoring, e.g. Routers, Switches, Firewalls, Windows OS, Application: Are you looking for one-time annual network/security consulting or ongoing log monitoring (i.e. LME/SIEM service)?
   ANSWER: This is an OPTIONAL service. We are seeking ongoing log monitoring.

5. **QUESTION:** How many policies, standards, and guidelines are to be included within the one review?
   ANSWER: This was answered in Amendment #3 question 7.

   QUESTION: For the Network Traffic Monitoring task, are you seeking a fixed price for this service? If so, please answer the following:
   ANSWER: This is an OPTIONAL service. Yes, we are expecting a fixed price.
   a. How often do you wish to conduct the monitoring – hourly, daily, weekly, etc.?
   ANSWER: We expect continuous monitoring of our edge network traffic, e.g. NetFlow, sFlow, J-Flow, PFIX. For reference, see the MS-ISAC Albert service (https://msisac.cisecurity.org/about/services/).

b. What actions do you want undertaken with the results?

ANSWER: We expect you to monitor for known bad addresses, hosts, and domains, and for other indicators that we may have been compromised.

c. Does the process exist or do you need to have one established?

ANSWER: The City has basic traffic monitoring in place, but we want something better. The City currently uses What's Up Gold for network traffic monitoring. What's Up Gold does not have the ability to analyze the traffic for threats. We manually review traffic for obvious issues. The City currently uses Trend Micro Deep Security for host based intrusion prevention. Trend does have the ability to detect, block, and alert on threats, but only for monitored hosts. We are seeking similar capability for our edge network traffic.

6. **QUESTION:** Is the risk assessment a review of the IT processes, procedures and controls that support the IT environment described in the Background section of the RFP? Or, does it also include technical security assessments of these technologies (e.g., firewall and network device configuration reviews, server configuration reviews, wireless network testing, etc.)?

ANSWER: Please refer to NIST Publication 800-30 "Guide for Conducting Risk Assessments". http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf. For requirement #1 "Risk Assessment" we are seeking a tier 1 and tier 2 scope, with a qualitative or semi-quantitative assessment approach, and an asset/impact oriented analysis approach. We expect to repeat this assessment process at least once every five (5) years. For requirement #11 "Project Advisory Services" we will request tier 3 "targeted" assessments for new systems, major changes, new threats, and new regulatory requirements.

http://www.wheaton.il.us/bids/

Attachments: None