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 #4

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

1. **QUESTION:** What processes do you use to collect credit cards? Web Applications? PC software? POS terminal? Please describe.
   ANSWER: Credit card payments are accepted through a PCI Council validated payment application published by Tyler Technologies that is installed on select cashiering workstations on our premises. Credit card payments are also accepted through the Govolution Velocity Payment Gateway -- Govolution is a wholly owned subsidiary of our merchant bank.

2. **QUESTION:** How many transactions are processed annually?
   ANSWER: We processed approximately 24,000 transactions last year. These transactions are split between Visa and MasterCard. We do not accept Discover or American Express. According to our merchant bank, we are a Level 4 merchant.

3. **QUESTION:** Do you store credit card numbers locally?
   ANSWER: No.

4. **QUESTION:** How many external IPs are connected to their Cardholder Data Environment (CDE)? If you have a web application (or web applications) that collects credit cards, how many IPs are involved?
   ANSWER: NONE - the only web application that accepts and processes credit card payments is the Govolution hosted Velocity Payment Gateway

5. **QUESTION:** How many IPs/hosts are part of the CDE internally? How many IPs/systems internally are used to collect and process credit card transactions? How many additional systems are in the same environment that do not process credit cards? Do you have documented policies for PCI?
   ANSWER: There are eight (8) IPs/systems internally that are used to collect, process, or transmit card holder data: primary firewall, standby firewall, and six (6) cashiering workstations. There are two (2) Cisco ASA 5505 VPN appliances in the CDE network. They are an active/standby pair that create a site-to-site VPN tunnel to our ERP software hosting datacenter -- card holder data is never transmitted to/from the ERP software, the ERP software only receives the payment amount and transaction confirmation number. We do have documented policies for PCI.

6. **QUESTION:** Number of in-scope, externally addressable systems (live IPs) across all locations
   ANSWER: Eleven (11) active IP's in a class C network space.

7. **QUESTION:** Number of in-scope, externally accessible web applications/sites
   ANSWER: None.

8. **QUESTION:** Number of in-scope critical systems (servers, routers, firewalls, etc. excluding desktops/laptops) (# of IPs) across all locations
ANSWER: There are approximately 125 critical systems (58 servers, 23 switches/routers/firewalls, 19 VoIP switches, and 25 UPS's).

9. **QUESTION:** Number of in-scope desktops/laptops across all locations
ANSWER: There are approximately four hundred (400) other devices, including desktops/laptops, VoIP phones, UPS's, and printers.

10. **QUESTION:** How many locations are in scope for wireless security assessment?
ANSWER: All tests can be performed from one (1) physical location. We use a Meraki wireless network which enforces a consistent configuration across all locations and AP's.

11. **QUESTION:** Are you interested in in-depth web application testing with credentials?
ANSWER: No.

12. **QUESTION:** Number of in-scope, externally accessible web applications/sites
ANSWER: N/A

13. **QUESTION:** How many "pages" with interactive inputs to test? (Please describe pages)
ANSWER: N/A

14. **QUESTION:** How many unique user roles
ANSWER: N/A

15. **QUESTION:** Which technologies / platforms / languages are being used?
ANSWER: N/A

16. **QUESTION:** What does the AP do?
ANSWER: N/A

17. **QUESTION:** Are you interested in in-depth, platform-specific security assessments? (Y/N - If yes, please answer the questions below): Number of in-scope infrastructure devices (routers and firewalls) across all locations
ANSWER: 3 (our primary firewall and our BGP router pair, currently a Cisco ASA5510 and two Cisco 2821's, but this equipment will be replaced within the next six months)

18. **QUESTION:** Number of in-scope Microsoft servers
ANSWER: 0

19. **QUESTION:** Number of in-scope Active Directory domains
ANSWER: 0

20. **QUESTION:** Number of in-scope virtual host servers
ANSWER: 0

21. **QUESTION:** Number of in-scope Linux and AIX servers
ANSWER: 0

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

Attachments: None