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 #3

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

1. **QUESTION:** Do each of the eight offices receive the same onsite internal services (i.e. PCI Cardholder Data Environment (CDE) Penetration Test, Internal Vulnerability Scan, etc)?
   ANSWER: Our network is composed of VLANs that span physical locations. We have only one PCI Cardholder Data Environment (CDE) VLAN. We have only one guest wireless VLAN. This network design allows us to perform all Internal scans and tests from a single physical location. PCI penetration testing will be conducted from one workstation VLAN and from the guest wireless VLAN. Internal vulnerability scanning will be conducted from one workstation VLAN and from within the public access television network (see question #2).

2. **QUESTION:** Could the City of Wheaton give an idea as to the scope of the Internal and External scans?
   ANSWER: For External scans, the City has a class C network 198.22.193.0/24. Although we only have eleven (11) active devices with external addresses, we do expect you to scan the entire class C network. For Internal scans, the City uses the class A private address space 10.x.x.x. This space is subnetted as a class B, and we use only the 10.0.x.x through 10.16.x.x networks. We only have about 500 active devices, and all of them are in the x.x.0.1 through x.x.2.255 client address space. The exceptions are our Azure network, which has two (2) hosts in the 10.0.3.0/26 network, and the public access television network, which has about forty (40) devices in the 192.168.5.0/24 network.

3. **QUESTION:** Are WiFi networks included in scope?
   ANSWER: WiFi networks are included in the scope of risk assessments and are used as a source for CDE penetration testing (see question #1). WiFi networks are not included in the scope of vulnerability scans.

4. **QUESTION:** Are the mobile devices included in scope of penetration testing and vulnerability scanning? How many are smartphones?
   ANSWER: Mobile devices are included in the scope of risk assessments. Mobile devices are not in the scope of penetration testing or vulnerability scanning. 52 of the City's 88 mobile phones are smartphones. We use Microsoft's Intune mobile device management program. We do not allow personal devices to connect to our Office 365 infrastructure.

5. **QUESTION:** Are any websites (i.e https://www.wheaton.il.us) included in the scope? How many external IP addresses are included within the scope?
   ANSWER: We do not code our own applications. We do not require any application specific tests or scans. See question #2 for the scope of External scans. See question #8 for currently outsourced scans.

6. **QUESTION:** Does training refer to high level training of IT staff - or is the training for general staff?
   ANSWER: Training refers to policy and security awareness training for end users. We conduct general training for all users and specific training for specific user roles, e.g. HR (HIPAA), cashiers (PCI), etc.

7. **QUESTION:** How many Policies, Standards and Guidelines are to be reviewed?
   ANSWER: Roughly a dozen.

8. **QUESTION:** Do you currently outsource any scans or tests?
   ANSWER: We use Trustwave for PCI external vulnerability scans and for file integrity monitoring of the cashiering workstations. We use Qualys for PCI internal vulnerability scans. We use the MS-ISAC for external vulnerability scans of our web site https://www.wheaton.il.us .

9. **QUESTION:** What risk management framework are you following?
   ANSWER: We have taken a blended approach based primarily on the NIST framework.

10. **QUESTION:** The background section of the bid package states that the city "…uses Azure…". What does this mean?
    ANSWER: We currently run two virtual servers in Azure that act as domain controllers and run Azure AD Connect. The intent of these servers is to ensure that our users can continue to login to Office 365 even if our on-premise domain controllers are unavailable. We are considering moving some of our critical workloads into Azure in the next fiscal year (May 1, 2017 through April 30, 2018). We will not make a decision on this until May. This is an example of a project for which we would seek advisory services from our cybersecurity consultant.

11. **QUESTION:** Where can I find the online directions for the call-in option for today's meeting? Is that where the answers to the questions asked today will be posted? Or will we receive the answers via email?
    ANSWER: Refer to the website link below and click on the RFP description to see all amendments and notices posted for this RFP. It is the vendor's responsibility to check the City of Wheaton web site to see if any additional amendments are issued regarding this project. Amendments may be issued until 48 hours before proposal due date.

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

Attachments: None