ADDENDUM 2

Request for Proposals

Managed Security Service Provider

******PROPOSAL DUE DATE CHANGE******

PROPOSALS WILL BE RECEIVED UNTIL

12:00 Noon, Friday, August 4, 2017

in

Purchasing Department, City Hall Building
101 North Main Street, Suite 324 Winston-Salem, NC 27101

July 25, 2017

Please acknowledge receipt of this Addendum and include with your proposal.

_____
Company

_____ _____
Authorized Signature Date

Questions/Responses

Questions as received with City responses:

- Is an extension to the due date available? **An addendum was sent out last week for an extension of a week.**
- What is the proposed timeline for deployment? **TBD based on vendor MSSP program**
- Is there a must-not-exceed date? **Not yet**
- What inter connectivity is there between all locations? Fiber Speed? 1GB (E.G. 100MB/s MPLS between all sites)
- Will there be anything added to the scope that is not listed in the RFP? **No**
- Please list the number of devices to be monitored on a per-location basis. **The majority of our infrastructure is located in our 2 Data centers with an interconnectivity of 20GB. The number of devices to be monitored will be based on the vendors MSSP program structure. This will allow the City to decide what services will be beneficial to the security posture.**
  - **Based on devices below *I would send the Security Infrastructure Monitoring & Management scoping doc details that show each category on how we can monitor.**
  - **Understand Tiers of support too**
  - CAT 1 -

- CAT 2 -
- CAT 3 -
- CAT 4 -
- CAT 5 -

- How much traffic does each site average in MBps? **Please explain in detail the reason for this request for information. If it is for pricing, respond with your pricing structure. We will provide more details to the winning vendors based on the total MSSP program.**
- Are the proposed Incident Response Times final, or can we propose our own? **The vendor should propose what they can deliver.**

We do have the ability to deploy our NetWarden virtually into the City of Winston Salem's existing virtual host infrastructure? **What are you asking?** Depending on client environment and distribution of assets this can provide substantial cost savings on deployment costs if virtual resources can be provided. Please indicate if and where this exists in your environment. **In the 2 Data Centers that is spelled out in the RFP.**

1. Does the City of Winston-Salem currently have in place any intrusion detection systems and if so what product / solutions? **No but The vendor provide recommendations based on their MSSP program.**
2. Does the City of Winston-Salem currently have in place any SIEM based technology or solution / service? If so what technology / solution / service? **No existing SIEM solution is in place.**

3. Does the City of Winston-Salem currently have in place any log management solution? If so what technology or solution? **Yes we have ePO. CWS cloud web filtering. Microsoft ATP. We capture ASA firewall logs, as well as all system logs.**

4. Does the City of Winston-Salem currently have in place any vulnerability scanning technology? If so what technology / solution / service? **Yes ePO.**

Detailed scoping questions below:

Note: …….. has made assumptions based on content provided in the RFP. We are asking the City of Winston-Salem to validate these assumptions and provide answers on all remaining questions.

On Premise:

- Approximate number of active systems:
  - Firewalls: **4 perimeter firewalls**
  - Switches: 2 (2 edge & 4 Nexus switches) ***2 edge switches and 2 Nexus 7009 routers***
  - Routers: **4 (2 edge & 2 internal routers)** ***2 edge routers 4 Nexus 5548 switches***
  - Windows Server 2008 R2: **Yes**
  - Windows Server 2012 R2: **Yes**
  - RedHat Linux 6x: **Yes**
  - Active Directory: **Yes**
  - Microsoft SQL Databases: **yes**
  - Oracle Databases: **yes**
  - Microsoft IIS server: **yes**
  - Apache application server:

  - Citrix Netscaler and hypervisor for VDI: ***2 internal virtual Netscalers and 2 external physical MPX Netscalers***
  - Microsoft DHCP: **Yes**
  - Microsoft DNS: **Yes**
- How many locations with dedicated internet ingress/egress need monitoring? **2**
  - **City Hall Main Data Center**
  - **A1a Secondary Data Center**
    - **(*Remote sites connect back to City Hall DC using MetroE wan circuits and fiber.**
- How many core switches are at each above location with dedicated internet? **1 at each location**

- Would you expect to see spikes of traffic higher than 700 Mbps for ingress/egress and host-to-host traffic at the above location(s)? **That would be rare if at all**

- Are there any systems within the City's seventy-four different, non-DC locations in scope for log collection/management? **No**
  - If so, how many locations and do they have VMWare at those sites? **Assume just City Hall and A1a Data Centers**

Perform regular wireless network security assessments. - Is regular once a year, twice a year, quarterly? What level/depth of security testing are they looking for?

- **Please explain to us your MSSP program and services. The vender must tell us the frequency outline in their program.**

- **The testing and depth should allow for no vulnerabilities to penetrate the City's infrastructure.**

Vendor Requirements
 Maintain all city collected data in a secure environment to be released by approved city staff.
Third Party - What is the required retention policy?

- Vendor should recommend based upon best practices.

 Using the vendor's proposed Security Information and Event Management (SIEM) solution provide reporting of all security events for infrastructure devices to also include user logins and password updates. Does CoWS require a SIEM?

- **The City requires what was outlined in the RFP.**

Is the vendor to provide firewall hardware as part of this service? **The vendor must recommend and/or provide all components that is needed to fulfill requirements outlined in the RFP.**

When you say eliminate security vulnerabilities, this is not something any vendor can do alone. This requires concerted efforts form the customer to patch and enable mitigating controls. What is the expectation of this statement? **This is a correct statement, hence the need of a MSSP that is mature enough to help the City security posture.**

Our solution will be near-real time is that acceptable? Transport and processing time of the SIEM platform are unavoidable.

- **Please respond to the RFP with your solution and set expectations of your proposed solution**

How often should "regular security assessments and auditing" be conducted. And what is the scope of the assessments and audiing?

- **The City is depending upon the vendor to make those recommendations.**

When you say "manage SSL certificates" do you mean implement and configure them? Or do you mean you want your provider to procure SSL certificates on your behalf? Also, what is the scope of this management?

- **This means identifying, tracking, inventorying expiration management, etc.**

Management of the log monitoring platform is not completely automated, is engineering support allowed in the solution proposal?

- **Please propose your solution and we will evaluate as outlined in the RFP**

When scaling to meet the City's requirements is the City okay with additional costs for service and potentially virtual infrastructure if the scaling exceeds the initial scope of deployment? Is the City okay with a cloud-based solution or is the City looking for an on-premise implementation?

- **Please propose your solution and we will evaluate as outlined in the RFP. We are open to either platform.**

"Troubleshoot infrastructure outages and problems" Does this mean you want the provider to troubleshoot internal City infrastructure outages and problems? This would require accounts and access to the City's infrastructure.

- **Specify your requirements in the proposal. Also as stated in the RFP the MSSP will work directly with the Network MSP for any security related issues.**

Are your notification SLAs flexible or firm?

- **Please propose your solution and we will evaluate as outlined in the RFP**

For reporting, are automated live dashboards acceptable or does the city require hardcopy or PDF reports?

- **The City must be able to print the reports.**
- **Please propose your solution and we will evaluate as outlined in the RFP**

What is the daily volume of data in Gigabytes that the City wants a vendor to ingest into a SIEM platform?

- **TBD based on the vendor proposed solution. Short answer is whatever it take to secure the City's infrastructure for Critical security vulnerabilities.**

ADDENDUM 2

1. What regulatory compliance laws and mandates is City of W-S operating under? Please list them

- PCI
- CJIS
- PII

2. Is City of W-S required to be PCI DSS v3.2 compliant in any capacity as a Merchant or Service Provider?

    - **Yes as a service provider for take payments**

3. Does City of W-S maintain personally identifiable information (PII) data of its customers?

    - **Yes**

4. Employee and customer security education and awareness is mentioned in the RFP Objectives but not in the SOW. Please list specific training needs, to which audience, and how often

    - **End user awareness training.**

5. When was the last security risk assessment conducted for City of W-S? Please describe the scope of this assessment.

    - **2014**
    - **Please propose your solution and we will evaluate as outlined in the RFP**

Monitoring:

1. Do you wish to have your endpoints monitored in addition to your servers?

- No

2. Can you forward the EPO logs to our system for correlation?

- **Yes**

Architecture:

1. Do you have and can you provide a logical representation of your network architecture?

- **We will provide details upon awarding a MSSP.**
- **Please propose your solution and we will evaluate as outlined in the RFP**

Does this include the wireless network segments? **Yes**
Do you currently have a WIPS?

- **No**

Trouble Ticketing System:

1. What is your trouble ticketing system?

    - **iVanti HEAT Classic**

2. What cross-reference function to you expect there to be?

    - **Looking for ticket integration.**

ADDENDUM 2

3. Is manual cross-reference capabilities sufficient?

   - **Please propose your solution and we will evaluate as outlined in the RFP**

4. Is there an API? **NO**

1.) Due to the timing of questions being due, answered, and subsequent deadline of Friday July 28th – is there a possibility of extending the due date for the RFP to allow adequate time to review question answers prior to submitting final version of response. **See addendum 1**

Is the city looking for a security controls risk analysis based on NIST, ISO, Sans, Etc? **Please propose your solution and we will evaluate as outlined in the RFP**

2.) Is the city looking for a security controls assessment based on NIST, SANs, ISO, Etc? **Yes the city is looking for a security controls risk assessment based on the vendor's recommendation.**
3.) Is the city looking for technical testing to validate the security of the network from an outside attempted intrusion (pen test)? **Yes this is a requirement in the RFP**.
4.) Do you currently have a patch/Endpoint management software such as CASE, LanDesk, Etc.? **Yes SCCM**
5.) Security Monitoring:
   a. Number of DNS servers
   b. Number of DHCP Servers
   c. Number of Domain Controllers
   d. Number of Active Directory Servers
   e. Number of Web Servers / Web Proxies

- **The city uses all the above and the details will be issuer to the successful vendor.**
- **Please propose your solution and we will evaluate as outlined in the RFP**

6.) Penetration Testing:
   a. What is the Number of Total ACTIVE IPs on the network(s) TBD

      - **TBD. Please propose your solution and we will evaluate as outlined in the RFP**

   b. What current compliance regulations (if any) you are seeking to adhere to? **PCI, PII, CJIS**
   c. Is there a current Security Framework? NIST, ISO, etc. **No**
7.) Is the city current utilizing Quarterly Vulnerability Scanning at minimum? **No**
8.) In reference to Continuous Vulnerability Scanning – Please provide:
   a. How many External (public Facing) IP Addresses?
   b. How many Internal (public Facing) IP Addresses?
   c. For internal scanning, do you prefer hardware scanning appliance or virtual machine (VM) based?
   d. Do you require Policy Compliance Scanning?

      TBD. Please propose your solution and we will evaluate as outlined in the RFP

   e. Do you require Web Application Scanning?

ADDENDUM 2

i. If yes to question 14, please include number of web applications being scanned

9.) Is the city required to adhere to any other compliance standards (PCI, HIPAA, Etc)? **NO**

10.) How many Access points/ Locations are available on your Wireless Network? **Over 250 AP's and as stated in the RFP there are 74 sites.**

11.) What is the estimated Number of City Employees and estimated number of laptops/desktops? **2500 employees est. 1500.**

- What security compliance framework does the City use? **None** Which controls are applicable per this RFP? **None**
- If NIST control framework, has a FIPS 199 categorization been established? **No** If so, what is the baseline for CIA? N/A
- The Objective section on Page 8 identifies several professional services items (i.e. environmental assessments, security awareness training, wireless network testing, eliminate security vulnerabilities (presumably through a patch management process), reviewing (and updating?) security plans, and perform regular auditing), however none of these are noted in the SOW requirements. Should they have been added as a requirement, or will this be add-on services we should offer separately?
  - **This will be determined via the vendors MSSP program and what and how it functions. The City is looking for a Vendor provide guidance to implement its security posture.**

Item 3:

- What is needed to cover Security Control Assessments?
- What controls need to be monitored and reported in the dashboard? **TBD based on the vendor's solution**
- Is the City asking for daily vulnerability scanning or pentests to be done, or just report if any are detected?
  - **The City is asking all vendors to provide responses to theier MSSP program. Again The City is looking for a Vendor provide guidance to implement its security posture.**

Item 4:

- What information sources are in-place for use in the 'security health comparisons?' **Logs from the ePO, CWS, Microsoft ATP, VMWare system logs, Linux system logs.**
- Is the vendor expected to add new security tools to provide alternative data sets? **Please provide your propose solution to meet the requirement outlined in the RFP.**

Item 6:

- What type of infrastructure outages are anticipated for the vendor to troubleshoot? For instance, does this include the City's routers, switches, etc. or does it just include outages associated with our SIEM and monitoring solution?
  - **This is a MSSP as stated in the RFP, The MSSP will work directly with the City's network MSP to resolve any security related events.**

What is the total number of egress points for the city?

- **City Hall Main Data Center**
- **A1a Secondary Data Center**
  - **(*Remote sites connect back to City Hall DC using MetroE wan circuits and fiber.**

ADDENDUM 2

What is the provisioned bandwidth for each egress point?
100 mbits/sec and 1 gb/sec

What is the % of utilization for each egress point?
40%

Is the city of ws using a vulnerability scanning product today? If so, who is the manufacturer, make, and version?
Yes ePO version 5.3

What is the total number of network security experts? Security analysts? Code developers? And IT staff (related to awareness training)
Maximum of 10

Is the city of WS currently using any forensic tools today? If so, who is the manufacturer, model, version?
No

Can the city of ws expand on the requirements related to securely storing logs?
The City will go with the recommendation of the MSSP.

Does the city follow any federal or industry standards related to this request? And are certifications required around PCI, CJIS, or FedRamp for this request?
PII, CJIS, PCI

Will the city provide an inventory list of devices that will be supported for security monitoring upon award of this request?
Yes

 Eliminate security vulnerabilities. This would only apply to security gear that was managed by the provider correct?

- **The testing and depth should allow for no vulnerabilities to penetrate the City's infrastructure.**