Request for Proposals

Managed Security Service Provider

Proposals will be received until

12:00 Noon, Thursday, April 22, 2021

Per Document Instructions

ADVERTISEMENT FOR PROPOSALS

Sealed proposals endorsed **Managed Security Service Provider** for the City of Winston-Salem will be received per document instructions by the City/County Purchasing Department **until 12:00 Noon, Thursday, April 22, 2021.** Instructions for submitting proposals and/or receiving the complete RFP document specifications may be obtained during regular office hours by contacting Jerry Bates via email jerryjb@cityofws.org **(Email is preferred)** or phone 336-747-6939. The City reserves the right to reject any or all proposals.

Jerry Bates
City/County Purchasing Director

This document **IS NOT** the complete proposal. To obtain the completed proposal specifications contact Jerry Bates via email jerryjb@cityofws.org or phone 336-747-6939.

INSTRUCTIONS TO PROPOSERS

INTRODUCTION:

This entire set of documents constitutes the RFP. The proposer should return the RFP with all information necessary to properly analyze the proposer's response in full. Proposer's notes, exceptions, and comments may be rendered on an attachment, provided the same format of this RFP text is followed.

Proposer Questions and Inquiries

Proposer Questions and Inquiries relative to this RFP must be submitted **in writing only by 12:00 Noon, Wednesday, April 14, 2021,** to Jerry Bates, City/County Purchasing Director, via e-mail: jerryjb@cityofws.org. The City will provide written responses to all inquiries received by this date, and responses will be made available to all recipients of this RFP. Any oral responses made by any representative of the City may not be relied upon. Any supplements or amendments to this RFP will be in writing and furnished to potential bidders.

RFP Response Submission

Bidders must submit Proposals electronically. To reduce printing costs and to facilitate recycling, we request that only electronic proposals in PDF format be submitted prior to the deadline. Electronic bids should be submitted by attaching a single file of the required bid forms to an email entitled, **"BID – Managed Security Service Provider – RFP21239**" and emailed to jerryjb@cityofws.org. This proposal **MUST** be received no later than **12:00 Noon, Thursday, April 22, 2021.** Such submission will not be opened until the time for receiving proposals has come. **Please do not wait until the last minute to send your Proposal to avoid any possible delay that may occur during the transmittal of files.** A screen print of the email receipt will be used by the City as verification of the time received. **Late proposals will not be considered.**

The City will not be obligated for the expenses of any provider arising out of preparation and/or submittal of responses to this RFP. Any and all proposals to this RFP are to be prepared at the cost and expense of the respondents, with the express understanding that there may be no claims whatsoever for the reimbursement of any costs, damages, or expenses relating to this procurement from the City or any other party for any reason (including the cancellation of this RFP).

Proposals must be made in the official name of the individual, firm, or corporation under which the business is conducted (showing official business address) and must be signed in ink by a person duly authorized to legally bind the business entity submitting the proposal.

All proposals should be complete and carefully worded and must convey all of the information requested by the City. If errors or exceptions are found in the proposal, or if the proposal fails to conform to the requirements of the RFP, the City will be the sole judge as to whether that variance is significant enough to reject the proposal.

Proposals should be prepared simply and economically. All data, materials, and documentation shall be available in a clear, concise form. The City reserves the right to reproduce proposals for internal use in the evaluation process.

Proposers are expressly forbidden from contacting any other city employee or city of Winston-Salem elected official regarding this Request for Proposals. Any such outside contact may result in disqualification from the request for proposal process.

The City reserves the right to hold proposals open for a period of ninety days (90) days after due date before making awards.

This document **IS NOT** the complete proposal. To obtain the completed proposal specifications contact Jerry Bates via email jerryjb@cityofws.org or phone 336-747-6939.

Managed Security Service Provider

INTRODUCTION

Introduction

City of Winston-Salem, NC (City) is accepting responses to this Request for Proposal (RFP) from qualified vendors to provide comprehensive information technology security and support services.

Objective

It is the City's intent to select a Managed Security Service provider (MSSP) that can demonstrate solid experience in delivering information security solutions that improve network security, strengthen governance, and support regulatory compliance. The proposal should include proactive security monitoring services, vulnerability assessment, penetration testing services, and comprehensive risk management reporting for two distinct City network environments.

- Implement a security operations center (SOC) and a security information and event monitoring (SIEM) solution.
- Implement real time data analysis and alerting of security events on the City's networks.
- Perform regular security assessments using industry accepted vulnerability scanning and penetration testing technology and methods.
- Provide automated compliance reporting that can be utilized for periodic audits.
- Participate in quarterly reviews covering the City's overall cyber security plan and overall system health.

Vendor Requirements

- Vendor must maintain all city collected data in a secure environment.
- Log collection, management, analysis must be automated. Vendor must provide detailed automation process documentation.
- Company must be ISO27001 certified.
- Vendor solution must scale as the City's infrastructure grows.
- Vendor's proposal must specify the number of in-house employees and any subcontracted staff.
- **NOTE: This RFP describes the City's proposed solution. All solutions will be evaluated.**
- **Note: Available budget not to exceed $100K per year for entire proposed solution.**

Administration

Format and Content

Proposals should respond directly to the Statement of Work. Failure to follow the prescribed format may result in a proposal being found noncompliant and therefore deemed unacceptable for further consideration.

Responses should be descriptive and include your approach to providing the requested services. Training, travel, licensing, and other required costs should be itemized.

Executive Summary

Each response shall include an Executive Summary that explains how the proposed solution meets the requirements indicated in this RFP. The Executive Summary shall be structured such that anyone reading only that section has a clear understanding of the proposed services.

The Executive Summary should address:

- A technical overview of the proposed solution for each of the requested services.
- The composition of the support team for each service, including any business partnerships.
- Summary of pricing for each service (see "Pricing" below).
- Method of connectivity between vendor's Security Operations Center (SOC) and City's network.

Certifications
List your Company's certifications and qualifications in the following technical specialties:

- Cisco Security Certifications – CCNA-Security & CCNP-Security
- GIAC Certifications
- CISSP
- Security +
- Any other cyber security relevant certifications.

Company Information

- Number of Engineers with the appropriate technical skills that will be assigned to this account. *Please list the specific certifications and qualifications of the assigned engineers.*
- Number and location of SOC(s).

Sub-Contractor Clause
In order to enforce strict cyber security controls and meet the requirements of this contract, Proposer shall not subcontract Proposer's duties within Services 1,3, and 5 under this contract. *Please specify if sub-contractors will be utilized for any services.*

References
Submit references from at least five current customers for which the vendor has been providing services of a similar nature as the services described in this RFP for at least 2 years.

Pricing
The vendor should submit pricing based upon the objectives listed in this document and the City's current enterprise architecture.

Note: Available budget not to exceed $100K per year for entire proposed solution.

Pricing should include any necessary software, hardware or configurations to support the listed objectives.

For each requested service, bidders must provide, if applicable:

- One-time startup costs the City will incur to begin using proposed solution.
- On-going costs that the City will incur for items or services necessary for the proposed solution, such as connectivity from vendor's SOC to City's network, software licensing, etc.
- Fee structure for supplemental services or recommendations outside of scope of this RFP. (ex. PCI compliance programs, training programs, professional services rates, etc.)
- Any shipping, travel, or other expenses related to the project.

Prices quoted in the vendor's proposal must be valid for at least 120 days after submission of the proposal to the City. All prices should be exclusive of sales tax.

The vendor should recognize that the City's infrastructure will change over time as older technology is replaced, equipment is decommissioned, or consolidated, and overall capacity of the infrastructure is expanded. The City reserves the right to adjust the quantity, configuration and composition of the equipment within the covered infrastructure over the term of the managed security services contract at the unit prices quoted in bidder's proposal. In addition, the City reserves the right to exclude one or more of the requested services from the winning bidder's contract on an item-by-item basis.

Should the City find services are not meeting the identified objectives, the City reserves the right to discontinue services by providing 30 days written notice.

Statement of Work

Requirements:

The following section describes the requested services that will be implemented to address security threats and vulnerabilities.

Item	Service	Tasks
1	Security Monitoring Service	• Security information and event management (SIEM) solution, with 24x7x365 monitoring and notification services provided by a security operations center (SOC). • A formal process for the maintenance, monitoring, and analysis of audit logs. • Alarm collection from deployed sensors. • Sensor profiling and base lining. • Develop correlation rules that trigger an alert for suspicious activity and/or security violations. • Provide reporting on security events and alerts. • Continuous monitoring of the SIEM application and triage outage, failure, negative trends or anomalies.
2	Troubleshoot and Initiate Corrective Action	• Begin problem diagnoses based upon SLA of trouble notification. • Alert City staff of security event. • Help identify root cause and provide findings report. • Work directly with City staff to resolve issues related to identified security events. • When requested, provide advanced support for troubleshooting highly complex security incidents until resolution and remediation is complete. • Provide post-incident forensic support.
3	Security and Compliance Reporting	• Automated compliance reporting that can be leveraged for periodic audits. • Provide use-case specific reporting as requested (PCI compliance, Firewall events, etc.).
4	Vulnerability Scanning and Penetration Testing	• Perform penetration testing of City's network at least once per year. • Perform vulnerability scanning of the City's network resources at least twice per year. • Provide findings and mitigation steps to resolve security vulnerabilities.
5	Quarterly Security Health Reviews	• Participate in quarterly reviews covering the City's overall security plan and overall system health. • Summary of month-to-month security health comparisons. • Review of security successes and failures. • Provide solutions to identified failures. • Recommend security best practices.

This document **IS NOT** the complete proposal. To obtain the completed proposal specifications contact Jerry Bates via email jerryjb@cityofws.org or phone 336-747-6939.

Service 1: Security Monitoring Service

The City will provide secure remote network access via VPN/SSH or other City approved protocol.

The City requires that the vendor must have an established Security Operations Center (SOC) that will provide continuous security monitoring and incident management on a 24x7x365 basis (i.e., 7 days a week, 24 hours a day, 365 days a year). The vendor's SOC will be staffed by senior level engineers to provide support, triage incidents, and engage the appropriate personnel and/or support providers. The support vendor is required to work with City staff to resolve any network security related problems. The City's infrastructure consists of two distinct air-gapped networks (Utilities SCADA and City IT Network) which contain approximately 375 servers (predominantly virtual), 950 PC endpoints, and 500 mobile tablet endpoints utilized across multiple network segments and physical locations.

Proposed Process

1. Vendor's security monitoring system detects an anomaly.
2. Vendor initiates an alert notification to the City as specified in a service level agreement which is based on severity and threat level.
3. If alert condition is determined to be of a critical nature, vendor will:
    a. Assign the trouble ticket to their qualified technical support engineer
    b. Send a corresponding alert notification e-mail to fixx@cityofws.org (which opens an internal trouble ticket)
    c. Initiate a phone call to the designated support staff member at the City

Service 2: Troubleshoot and Initiate Corrective Action

Service Window

The City requires that the vendor 1) provide troubleshooting and corrective action services on a 24x7x365 basis (i.e., 7 days a week, 24 hours a day, 365 days a year), and 2) will follow the City's change control process.

Proposed Process

1. A new trouble ticket can be initiated by the vendor's security monitoring service or from a call to the vendor's help desk by a member of the City's IT support team.
2. The vendor's technical support engineer will attempt to diagnose and resolve the reported problem remotely.
3. The vendor will communicate and provide failure diagnostics and/or failure correction tasks to City's IT support team.

Incident Response Time

It is the City's expectation that the vendor will operate within the following response times for all trouble tickets:

Level	Description
● P1 / Critical	An Incident identified either by automated correlation rules or through SOC analysis that is deemed to be an ACTIVE threat against business impacting customer assets.
● P2 / High	An Incident identified either by automated correlation rules or through SOC analysis that is deemed to be a PROBABLE (current, possible impact) threat against business impacting City assets.
● P3 / Medium	An Incident identified either by automated correlation rules or through SOC analysis that is deemed to be a POTENTIAL (not current, may have future impact) threat against business impacting City needs.
● P4 / Low	An Incident identified either by automated correlation rules or through SOC analysis that may require further investigation, with no apparent threat against business impacting customer assets.

Severity	Action	Monitoring Targets
● P1 - Critical	Acknowledgment*	Within 15 minutes
	Response time**	Within 15 minutes
	Escalation to Management	Within 2 hours
● P2 - High	Acknowledgment*	Within 30 minutes
	Response time**	Within 30 minutes
	Escalation to Management	Within 4 hours
● P3 - Medium	Acknowledgment*	Within 1 hour
	Response time**	Within 2 hours
	Escalation to Management	Within 24 hours
● P4 - Low	Acknowledgment*	Within 2 hours
	Response time**	Within 4 hours
	Escalation to Management	As Required

Service 3: Security and Compliance Reporting

Proposed Process

The Vendor should provide role-based access to collected data via a secure customer portal. The vendor should provide historical reporting on the deployed security measurements and retain that data for a minimum of 3 years. Report data should be available in both .PDF or .XLSX formats. It is expected that the vendor will at minimum produce an analysis of at least the following factors:

- Reporting on captured security events
- Reporting on alerts generated from deployed correlation rules
- Automated compliance/non-compliance reports
- Custom specific use-case reporting (PCI, Audit, Firewall Summary Reports, etc.)
- Service Level Agreement Compliance

Vendors are requested to provide a sample of their historical trend reports in their response, and a list of any additional canned reports that are available in their proposed solution.

Service 4: Vulnerability Scanning and Penetration Testing

Proposed Process

The Vendor will be expected to conduct annual penetration tests and vulnerability scanning of the City's network resources to ensure that the City's cyber security controls are working effectively. Reporting of the findings and mitigation steps to correct any vulnerabilities will be presented to City staff during a Quarterly Security Health Review. Again, we have two distinct networks that may have to be done differently based on compliance and system requirements, schedules, etc.

Service 5: Quarterly Security Health Review

Proposed Process

The Vendor will be expected to participate in a quarterly review of the statistics captured by historical reports of the monitored services over the previous three months. The purpose of the review is to provide security successes and failures and month to month security health comparisons for future planning and corrective actions. Vendor will assist with review of cyber security related policies and procedures and provide best practice recommendations to strengthen the City's cyber security controls.

Appendix A

The following is a summary of the City's Information Systems network standards and architecture:

Category	Function	Standard
Network	Communication Protocol	TCP/IP OSPF MPLS
	Ethernet Wireless	IEEE 802.3u, IEEE 802.2 802.11 802.11a, b, g, n, ac
	Cabling	Multimode fiber Singlemode fiber Cat. 5e / Cat. 6
	DNS/DHCP	Windows 2008 R2 / 2012 R2, 2016
Management	Network Mgmt	SNMP, Cisco NCS Prime Infrastructure, Cisco EPNM Active Directory (AD), Insight
	Security	LDAP, AD, SSL Certificates (HTTPS), ACL's, McAfee ePO desktop, Cisco firewall, Cisco Umbrella Web Security/AMP
	Application Mgmt / Agents Printer Mgmt File Mgmt	SNMP agents, Tidal software Sysadmiral Web jet Admin, Ricoh DMNX Microsoft AD, OneDrive
	Desktop Management	SCCM, McAfee ePO Enterprise Policy Orchestrator Server
	Source Code	MS Visual Studio/Team Foundations
	Support / Change Control /Customer Support Center	iVanti HEAT Ticketing System
	Virus Protection (Windows)	Cisco AMP, McAfee VirusScan Enterprise
	Backup Solution	Veritas Netbackup, Storage TEK tape library (DLT/LTO), Veeam Backup & Replication
	Mass Storage	RAID, SAN, NAS (NetApp) ISCSI, Fiber Channel
Database	Enterprise	RDBMS (Oracle, MS SQL)
	Workgroup	RDBMS (Oracle, MS SQL)
	Standalone	RDBMS (MS Access)
Work Flow	Business Process Mgmt	Metastorm eWorks
eCommerce / Web		IIS, Tomcat
	Communication Protocols	HTTP, HTTPS, FTP, SSH
	Content Management	DotNetNuke (DNN)
	Content	HTML, CSS, CGI, JavaScript, JavaBeans
	Database Access	ActiveX, XML, ASP, ASP.NET, JavaVM, J2EE Java Servlets
Geographic Information System	Spatial Data Management	ESRI (ArcGIS, ArcIMS, ArcSDE)
Office Applications	Email	Microsoft O365/Outlook, IMAP 4 (POP3 compliant), SMTP

Category	Function	Standard
	Project Management	Microsoft Project 2013/16
	Word Processing, Spreadsheet, Presentations, etc.	Microsoft Office 2013/16
	Virus Protection	Cisco AMP, McAfee VirusScan 8
	Browser	Internet Explorer 11/Edge, Firefox, Chrome
	PDF Reader	Adobe Acrobat/Edge
Platform / OS	Enterprise Server	Cisco UCS Blades, Windows 2008 R2 and Windows 2012/2016 Advanced Server ESX VMware Virtual Server
	Desktop	Windows 7 / Windows 10
	Workstation	Windows 7 / Windows 10 (Minimum P4, 3.8GHz, 2GB RAM, 250 GB FXDD)
	Laptop	Windows 7 / Windows 10 (Minimum Pentium M, 1.6MHz, 512MB RAM, 60 GB FXDD)
	Hand-held Computer	iPad, HP Windows 10 tablet
Printers	Networked Print Server	Ricoh MFP Internal HP JetDirect with HP LaserJet (B/W, Color, MFP)
	Workgroup Color	Ricoh MPC 3503
	Standalone	HP DeskJet or LaserJet Series
	Plotter	HP DesignJet Series

Please see a listing of FAQ with City responses at the end of this document that may be helpful

This document **IS NOT** the complete proposal. To obtain the completed proposal specifications contact Jerry Bates via email jerryjb@cityofws.org or phone 336-747-6939.

Proposal Evaluation

As part of the evaluation process, the Evaluation Panel, consisting of City Staff, may engage in discussions with any Proposer. Discussions might be held with individual Proposers to determine in detail the Proposer's qualifications, to explore with the Proposer the scope and nature of the required contractual Services, to learn the Proposer's proposed method of performance and the relative utility of alternative methods, and to facilitate arriving at a contract that will be satisfactory to the City.

Since the City may choose to award a contract without engaging in discussions or negotiations, the Proposals submitted shall define the Proposer's best offer for performing the services described in this RFP.

Selection Process

Proposals will be evaluated for quality, completeness, and price value to the City of Winston-Salem by an Evaluation Panel. Selection shall be made from all offers deemed to be fully qualified and best suited among those submitting proposals based on the evaluation of factors included in the RFP, including price. Price shall be considered but need not be the sole determining factor. The Evaluation Panel may cancel this RFP or reject proposals at any time prior to an award and is not required to furnish a statement of the reason why a particular proposal was not deemed to be the most advantageous.

The City reserves the right, as part of the selection process, to request on-site (or virtual) demonstrations and/or presentations. In the event that such demonstrations or presentations take place, proposers will be selected for this process based on scores derived from the scoring matrix, which includes M/WBE participation, local availability, and all other applicable criteria. The scoring of the demonstration or presentation must be based upon the criteria from one or more of the original evaluation factors. After the demonstrations or presentations, each proposer will then be re-graded on the same criteria. The number of proposers chosen to take place in the demonstration/presentation process is subject to administrative discretion.

Evaluation Criteria

Below is a description of the evaluation criteria that will be used to evaluate the proposals. To be deemed responsive, it is important for the firm's proposal to contain appropriate detail to demonstrate satisfaction of each criterion and compliance with the performance provisions outlined in this RFP. The proposal will be the primary source of information used in the evaluation process. Proposal must contain information specifically related to the proposed services requested in this RFP. Failure of any firm to submit information requested may result in the elimination of the proposal from further evaluation.

Respondents will be evaluated for selection on the basis of the Proposer most qualified to meet the requirements of this RFP. Major criteria to be considered in evaluation may include, but shall not necessarily be limited to:

- **M/WBE Commitment:** Proposer's efforts to comply with all the terms and conditions of the City of Winston-Salem's Minority and Women Business Enterprise (M/WBE) Program through award of subcontracts to minority and women-owned business enterprises and utilization of minority and women owned business enterprise suppliers to the fullest extent consistent with the efficient performance of this contract. **If an entity is certified as a Minority Business by a state other than North Carolina, proof of certification must be submitted with the proposal.**

- **Location of Business:** "Location of Business: In order for the proposer to receive points allocated for location of business, the proposer shall submit the required documentation to comply with provision A (Winston-Salem/Forsyth County presence) or provision B (North Carolina presence) determined by the physical location of the firm (P.O. Box does not qualify).

  (A) Presence in Winston-Salem/Forsyth County: Proposer must have a physical office within the corporate limits Winston-Salem (P.O. Box does not qualify). For proposals submitted to a City/County joint department, a physical office within Forsyth County is acceptable (P.O. Box does not qualify). In order to determine a proposer's presence/location within Winston-Salem or Forsyth County, the proposer or at least one of the proposer's employees must have a physical office location in Winston-Salem or Forsyth County and **the proposer shall submit under confidential cover with his/her proposal, evidence that as the employer, the proposer has paid payroll taxes for the firm located in Winston-Salem or Forsyth County for at least one employee, (i.e. North Carolina Income Tax Withholding Form with receipt**

for payment). Said employee(s) must work in an office, which may be an office physically located within the employee's home in Winston-Salem or Forsyth County. If it is a home office in Winston-Salem or Forsyth County, then the proposer shall also submit with his/her proposal, evidence of a valid home occupation permit for said office, or evidence that said home office is not in violation of any zoning requirements in the event the applicable city does not require a home occupation permit.

(B) Presence in North Carolina: Proposer must have a physical office within North Carolina (PO Box does not qualify). In order to determine a proposer's presence/location within the State of North Carolina, including Winston-Salem or Forsyth county, the proposer or at least one of the proposer's employees must have a physical office location in North Carolina and **the proposer shall submit under confidential cover with his/her proposal, evidence that as the employer, the proposer has paid payroll taxes in North Carolina for at least one employee, (i.e. North Carolina Income Tax Withholding Form with receipt for payment)**. Said employee(s) must work in an office, which may be an office physically located within the employee's home in North Carolina. If it is a home office in North Carolina, then the proposer shall also submit with his/her proposal, evidence of a valid home occupation permit for said office, or evidence that said home office is not in violation of any zoning requirements in the event the applicable city does not require a home occupation permit.

Failure to include evidence of paid payroll taxes for firms located in Winston-Salem, Forsyth County, or North Carolina for at least one employee and a valid home occupation permit, if applicable, with the proposer's response, will result in zero (0) points being awarded for location of business."

- **Functionality and Capability:**
  Does the proposal describe an overall solution architecture that will fully support the security monitoring and support functions and protections requested by the City? Are requirements appropriately addressed in the vendor's responses? How well has the vendor demonstrated a methodology to deliver the project as specified in this RFP and be responsible for the overall project deliverables? Does the proposal articulate a clear understanding of the needs and expectations related to the project?
- **Relevant Qualifications:** Proposal describes relevant qualifications and experience of the personnel who will be assigned to the project. Service Providers will be evaluated on the background and experience information provided in this RFP. Proposers should submit completed "Staff Qualifications Proposal Form" with proposal.
- **Cost Effectiveness/Price Value:** Reasonableness/competitiveness of proposed fee and/or benefits to the City of Winston-Salem although the Evaluation Panel is not bound to select the respondent who proposes the lowest fees or most benefits for services. The Evaluation Panel reserves the right to negotiate fees and/or benefits to the City of Winston-Salem with the selected respondent(s).
- **Relevant Experience:** Proposal describes relevant experience and demonstrated ability to fulfill the requirements of the proposal as listed in the scope of work, Service Providers will be evaluated on the background and experience information provided in this RFP. Proposers should submit at a minimum five (5) verifiable references, preferably ten (10), for similar services performed within the past two (2) years, preferably with governmental entities. Ten (10) references would be graded higher than five (5) verified.

The following "Weighted Scale" will be used to evaluate each proposal.

Evaluation Criteria	Weight
MWBE Commitment	20.00
Business Location	20.00
Functionality / Capability	30.00
Relevant Qualifications	15.00
Cost Effectiveness/Value	5.00
Relevant Experience	10.00

Frequently Asked Questions

Question: Does the City of Winston-Salem currently have its own SIEM or will we price it out in the proposal?
Response: The City currently does not have a SIEM solution in place and is requesting pricing on a vendor managed SIEM or "SIEM like" solution.

Question: Can you provide a bit more information on the Penetration Testing. Is it internal or external?
Response: The City is requesting pricing on both internal and external pen testing. Our requirements for internal pen testing is limited to a small group of machines/servers mainly for PCI compliance needs. Our external pen testing requirements include our public facing web servers and edge gateways/firewalls

Question: Will any of the 950 PC endpoints or 500 mobile tablet endpoints leave the City's network? Such as a 4G connection or other wifi network?
Response: Yes. Of the 950 endpoints, some are mobile laptops. Most of the 500 tablets are 4G connected.

Question: Does the vendor need to qualify either part A or B of Location of business on Page 9 (found in the advertisement) in order to submit a proposal?
Response: **No -** The vendor does not need to "qualify" either part A or B of location of business but would not receive any point value toward their total scoring **–** a vendor may still submit a proposal for consideration.

Question: Will the city provide the vendor with the necessary administrative rights to network devices and servers in order to diagnose and resolve a reported problem?
Response: Selected vendor will be given the appropriate rights to perform the tasks included under the contract of services.

Question: What do you use for Single Sign On and/or Identity?
Response: ADFS 4.0

Question: What is the scope of the automated compliance reports? To which framework is compliance requested?
Response: No required scope. Depth of automated reporting functionality will be evaluated from each proposal/solution.
Question: Internal Pen Testing – how many IPs are in-scope?
Response: Up to 100
Question: External Pen Testing – how many IPs are in-scope?
Response: Up to 250

This document **IS NOT** the complete proposal. To obtain the completed proposal specifications contact Jerry Bates via email jerryjb@cityofws.org or phone 336-747-6939.