File #: 20-0213, **Version:** 1

TO: Mayor Richard C. Irvin

FROM: Michael R. Pegues, Chief Information Officer
David Schumacher, P.E., Superintendent Water Production Division
Leela Karumuri, IT Risk & Compliance Manager

DATE: March 16, 2020

SUBJECT:
Requesting approval of professional services in the amount not to exceed $89,989 to perform cyber remediation with 1898 & Co., Part of Burns & McDonnell for the Water Treatment Plant SCADA system to enhance the security posture of critical infrastructure in the City of Aurora.

PURPOSE:
This Requesting acceptance of the winning response for the Request for Qualifications RFQ# 19-77 Cybersecurity for Critical Infrastructure, Water Treatment Plant Cyber Remediation:

-Publication Date/Time Phase 1: 11/21/2019
-Publication Information: Aurora Beacon News and Demand Star
-Marketplace.city Clear Box Review
-Closing Date/Time Phase 1: 12/06/2019
-Submission Info: Thirty one bids/solicitations were submitted to the City of Aurora.
-<https://www.aurora-il.org/bids.aspx?bidID=208>
-<https://hubs.ly/H0n5ksT0>

-Publication Date/Time Phase 2: 12/17/2019
-Marketplace.city Clear Box Review
-Closing Date/Time Phase 2: 01/18/2020
-Submission Info: 14 bids/solicitations were submitted to the City of Aurora.
-<https://hubs.ly/H0n5kS30>

-Disclosed the vulnerabilities through encrypted emails as Phase 3:
-Meeting with final 5 vendors through conference calls and onsite visits to assess capabilities from 02/07/2020 to 02/11/2020.
-Last date to submit the pricing by noon 02/17/2020.

BACKGROUND:
As part of the City of Aurora Technology Strategic Plan or “IT Roadmap” for 2019, the Information Technology Division is seeking to evaluate and improve Governance and Security citywide.

This strategic line of defense and arguably the most important, will be for the City to establish and

maintain a comprehensive Cybersecurity for all Critical Infrastructure.

The City is seeking information and quote to perform a cyber remediation for the City owned water treatment plant SCADA system. A cyber assessment was performed and report issued in December of 2018. The City wants to follow through on those recommendations and began to plan and prioritize remediation activities.

The City wants a partner to create full remediation plan and implement High and Medium priority remediation in the first phase. The City is seeking to understand interested parties' capabilities, public sector experience and pricing. Companies matching their criteria will be invited to review for detailed information, finalize scope and finalize pricing.
The statement of work includes:

Phase 1- Project Data Review

Overview: This phase will start with gathering, exchanging, and reviewing information relative to the systems in scope.

Deliverables:

Perform site walk through
Conduct key requirements/success factors workshop
Summary results from the site visit
Potential "quick win" remediation

Potential approach:

Existing Data Review:

Detailed review of all available documentation pre-site visit. These include current network drawings, asset inventory list (Windows assets, managed switches, firewall, PLC racks, smart devices/instruments), IP address list and VLAN scheme, policies and procedures (backup and recovery, MOC, remote access)

Site visit:

Conduct walk through of the site including server rooms, control rooms, rack rooms, field I/O cabinets, MCC room, etc.
Requirements workshop - Conduct a workshop to discuss key requirements/success factors for the remediation measures including existing network layout, planned modifications to be considered, engineering/maintenance user requirements, change management, administration and management of the remediation solutions, etc.
Document results of the site visit

Phase 2- Detailed Design and Planning

Overview: Based on the information from the prior evaluation and gathered from the Phase 1,

develop a detailed mitigation plan including conceptual design and delivery schedule.

Deliverables:

Design of the proposed remediation measures including process and change management
Confirm scope of work and any outside hardware, software, services for remediation
Confirmation of budget and timeline for delivery of remediation steps
Initial “quick win” delivery of remediation from assessment

Current High and Medium Priorities Remediation

SCADA Network Segmentation and Optimization (including SCADA DMZ and Domain)
SCADA Firewall Review and Rationalization
SCADA Patch Management Solution
Backup/Recovery - Short term solution using existing tools
SCADA Application Whitelisting and/or Antivirus solution
SCADA Asset/Vulnerability Management solution
Secure SCADA remote access solution
Backup/Recovery - Standardized and automated solution leveraging asset management products/solutions tailored for the ICS environment

Potential Activities:

For each of the above remediation
Create project plan outline, scope, timeline and external costs
Create sequencing for remediation steps
Confirm owner and deliver lead for each step (city, vendor, etc.)
Remediation specific activities as needed

Phase 3 - Implementation

Overview: With confirmed scope and budget, implement and deliver the agreed upon high and medium remediation.

Deliverables:

Deliver remediation plans and activities as agreed upon in prior steps

Potential approach

Provide onsite support for configuration and commissioning
Provide onsite training for administration and maintenance of the solution
Technical support as needed
Coordinate with 3rd party vendors as needed per the scope

Phase 4- Governance, Documentation and Policy (can be delivered with Phase 3 if applicable)

Overview: Assist city in developing their SCADA cybersecurity program materials.

Deliverables:

Policies and procedures benchmarking
Development of ICS specific policies and procedures
Risk management process
Role based training program
Incident Response Plan for ICS specific use cases

Potential Approach:

SCADA cybersecurity framework, policies and procedures
Review policies and procedures including those currently existing for the office network and identify core set of documents to be developed/modified for the SCADA control system.
SCADA risk management procedure
Develop a risk-based approach to assess, manage and maintain the SCADA system network and assets.
SCADA security training program
Develop a role-based training program for ICS cybersecurity awareness and training that is tailored for the SCADA control system engineering, operations and maintenance
SCADA incident response plan (IRP) develop an IRP for ICS specific use cases leveraging existing corporate level IRP and business continuity plans.

DISCUSSION:
The City of Aurora, Purchasing Division, 44 E. Downer Place, Aurora, IL 60507 sent an RFQ on 11/21/2019.

Local preference does not apply to this Request for Qualifications.

Phase 1 RFQ: Provided general information regarding the cybersecurity/network vulnerability test/remediation for critical infrastructure from eligible vendors and received 31 bids. Then selected 14 vendors with critical infrastructure cyber security experience in the public sector.

Phase 2 RFQ: Selected 5 vendors with proven experience in cyber security of Operational Technology (OT)/SCADA system. <http://www.uky.edu/WDST/SCADA.html>

Phase 3: Contacted final 5 vendors for interviews, onsite visits and or conference calls.

IT Division Cybersecurity & Operation staff quantified technical requirements and fit for use based on the following evaluation scoring matrix:
Company Capabilities - 26%
Qualifications and Staffing - 20%
Services and Implementation Methodology - 12%
Pricing and Contract - 18%
Value added services and others - 24%.

5 vendors reached final pass of the three phase RFQ process and ranked as follows:

1898 & Co., Part of Burns & McDonnell
AESI-US, Inc.
Sentinel Technologies
Applied Engineering Solutions, Inc.
Electric Power Systems-Engineering & Design

FIRST PASS: (2) Both Applied Engineering Solutions Inc. and Electric Power Systems Engineering & Design were eliminated who scored less than 80%. Although EPS Engineering & Design offering better pricing, they scored lower for the other requirements like company capabilities and value added services. Applied Engineering Solutions pricing is $1,15,8830.00 which is not acceptable and does not have proven experience with public sector projects.

SECOND PASS: (2) AESI-US, Inc. and Sentinel were eliminated who scored less than 90%. These vendors scored reasonably well on company capabilities, qualifications and implementation methodologies. Nevertheless, we had to consider their company capabilities for cyber security of critical infrastructure, in terms of scale and scope, therefore they did not advance to the final pass. Sentinel has provided excellent professional services to the City of Aurora for years, but they are experts in IT but their cyber security practice in Critical Infrastructure is at early stages of development and lacks a proven track record.

THIRD PASS: 1898 & Co., Part of Burns & McDonnell scored more than 90% and reached the final pass. They were identified and selected as the top scorer with 96%. Their study and understanding threat actors for Critical Infrastructure with coupled extensive engineering foundation across multiple sectors make them an outstanding choice against all other vendors. Their approach to vulnerability assessments and remediation strategies is rooted in a simple, efficient, and effective method utilizing proven real-world technical experience combined with their comprehensive understanding of industry best practices. The flexibility of the methodology allows us to assess and improve our organization's security posture across a variety of practices, standards, and regulations within multiple business sectors such as Energy, Water, Communications, and Defense. Their value-added services offering added points to selection process.

We strongly believe 1898 & Co.; Part of Burns & McDonnell provides the ability to propel the City of Aurora forward into secured city with cyber secured critical Infrastructure.

Funding for this purchase comes from 2019 DP and 2020 DP -

Amount carried over to 2019 from 2020 - computer/software applications
Acct # 510-1380-511.64-11) - $73,000.00

Budgeted amount for 2020 - computer/software applications
(Acct # 510-1380-511.64-10) - $40,000.00

Budgeted amount for 2020 - Professional fees/contracted services
(Acct # 510-1380-511.32-20) - $30,000.00.

Total budgeted amount not to exceed: $143,000.00

IMPACT STATEMENT:
N/A.

RECOMMENDATIONS:
Requesting approval of professional services in the amount not to exceed of $89,989 to perform cyber remediation with 1898 & Co., Part of Burns & McDonnell for the Water Treatment Plant SCADA system to enhance the security posture of critical infrastructure in the City of Aurora.

cc: Infrastructure & Technology Committee

CITY OF AURORA, ILLINOIS

RESOLUTION NO. _____
DATE OF PASSAGE _____

A Resolution authorizing approval of professional services in the amount not to exceed of $89,989 to perform cyber remediation with 1898 & Co., Part of Burns & McDonnell for the Water Treatment Plant SCADA system to enhance the security posture of critical infrastructure in the City of Aurora.
WHEREAS, the City of Aurora has a population of more than 25,000 persons and is, therefore, a home rule unit under subsection (a) of Section 6 of Article VII of the Illinois Constitution of 1970; and

WHEREAS, subject to said Section, a home rule unit may exercise any power and perform any function pertaining to its government and affairs for the protection of the public health, safety, morals, and welfare; and

WHEREAS, this service was to provide safest, cleanest drinking water to the City's residents. The City of Aurora has control systems assets that are critical to the production of drinking water for the community, and

WHEREAS, the City published the Request for Qualifications for this project on November 21, 2019; and

WHEREAS, the plan is to implement cyber remediation to the vulnerabilities assessed before on Water Treatment Plant and secure essential services with potential and significant consequences to the city and its customers by any intentional or unintentional cyber incidents, and

WHEREAS, funds are available in accounts:
$40,000 510-1380-511.64-10 - Computer/software applications
$73,000 510-1380-511.64-11 - Computer/Hardware applications

$ 30,000 510-1380-511.32-20 - Professional fees/contracted services; and)

NOW, THEREFORE, BE IT RESOLVED by the City Council of the City of Aurora, Illinois, as follows: requesting approval of professional services in the amount not to exceed of $89,989 to perform cyber remediation with 1898 & Co., Part of Burns & McDonnell for the Water Treatment Plant SCADA system to enhance the security posture of critical infrastructure in the City of Aurora.