SUBJECT:

Requesting approval to procure professional services for IT Risk Assessment, development of National Institute of Standards and Technology (NIST) 800-53-1 Policies and Incident Response Plan to heighten the security of the information systems and critical infrastructure used within the City of Aurora government. Total amount should not exceed $86,000.

PURPOSE:

Requesting acceptance of the winning response for the Request for Qualifications (RFQ) 19-03: Managed Security Services for Risk Assessment, Policy Development and Incident Response Plan for the Information Technology Division.

- Republication Date/Time: 04/26/2019
- Republication Informaton:Aurora Beacon News and Demand Star
- Closing Date/Time: 05/13/2019
- Original Publication Date/Time: 1/23/2019 12:00 AM
- Orginial Publication Information: Aurora Beacon News and Demand Star
- Orginal Closing Date/Time: 2/13/2019 12:00 PM
- Submission Info: Twenty Seven bids / solicitations were submitted to the City of Aurora, Attn: Purchasing Division, 44 E. Downer Place, Aurora, IL 60507. For more information: https://www.aurora-il.org/Bids.aspx?bidID=131

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 Plan. This initiative affects all stakeholders; therefore, planning efforts need to be comprehensive, and will include the following actions:

- Perform a security baseline / risk assessment
- Determine business requirements and mission compliance requirements
- Design, build and implement a governance framework
- Define and implement information security policies, standards and procedures

The Statement of Work includes:

1. CYBERSECURITY RISK ASSESSMENT:

Vendor will conduct a Cybersecurity Risk Assessment of City's infrastructure which will consist of an assessment of the following three areas:

- People
- Process
- Technology

The Cybersecurity assessment should also include a NIST 800-30 based Risk Assessment and threat analysis at the Organizational, Business Process, and Information System levels for City which will focus on the following:

- Detailed analysis of various threat occurrences, both the potential and the impact of the threats occurring.
- Detailed analysis of the level of risks for these threats in order of highest priority.
- Detailed analysis of recommended short, medium, and long-term remediation efforts to resolve identified threats.

CYBERSECURITY ASSESSMENT TASK DELIVERABLES:

The deliverables for this task is detailed in the attachment – 19-03 RFQ MSS Risk Assessment Policy Development Incident Response Plan.doc in Legistar.

2. NIST 800-53-1 POLICY DEVELOPMENT:

Vendor will develop the following policies NIST 800-53 (-1 Controls) policies:

- Access Control
- Audit and Accountability
- Awareness and Training
- Security Assessment and Authorization
- Configuration Management
- Contingency Planning
- Identification and Authentication
- Incident Response
- Maintenance
- Media Protection
- Personnel Security
- Physical and Environmental Protection
- Planning
- Risk Assessment
- System and Communications Protection
- System and Information Integrity
- System and Services Acquisition

Vendor will work with City Senior IT Management to define the organizational defined values that should be stipulated in each NIST policy.

Vendor will work in conjunction with City to define the timeline for development, review, editing, and completion of each policy.

POLICY DEVELOPMENT TASK DELIVERABLES:

The deliverables for this task will be the following NIST 800-53-1 Rev. 4 policy documents:

- Access Control
- Audit and Accountability
- Awareness and Training
- Security Assessment and Authorization
- Configuration Management
- Contingency Planning
- Identification and Authentication
- Incident Response
- Maintenance
- Media Protection
- Personnel Security
- Physical and Environmental Protection
- Planning
- Risk Assessment
- System and Communications Protection
- System and Information Integrity
- System and Services Acquisition

3. INCIDENT REPONSE PLAN

Vendor will develop an Incident Management Plan for MEC which will define a general framework to be used for managing declared incidents. The framework of the plan will consist of the following components:

- A guiding framework for conducting triage activities before and after an incident is declared.
- A guiding framework for conducting incident response activities after an incident is declared.
- A guiding framework for conducting incident containment activities.
- A guiding framework for conducting incident eradication activities.
- A guiding framework for conducting incident recovery activities.
- A guiding framework for establishing and managing communications and crisis management during an incident.
- MEC IT Key Points of Contact Definitions.
- Conduct a general review of MEC Information systems/assets, Locations.
- Conduct a general review of MEC info sec monitoring/logging capabilities
- General definition of MEC affiliated third party resources available to assist with response activities (ex. Technology support contract resources)
- Detailed review of all contractually based incident response service level agreements.

INCIDENT RESPONSE DEVELOPMENT DELIVERABLES:

The deliverables for this task is detailed in the attachment – 19-03 RFQ MSS Risk Assessment Policy Development Incident Response Plan.doc in Legistar.

DISCUSSION:

The City of Aurora, Purchasing Division, 44 E. Downer Place, Aurora, IL 60507 received a total of 25 bids and cost proposals in two separate, individually sealed envelopes by 12pm, Monday, May 13, 2019.

Upon receipt, the 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 –24%
- Value added services and others – 18%

FIRST PASS: (10) vendors were eliminated who scored less than 85%. Although certain vendors offering better pricing, they scored lower for the other requirements like *company capabilities* and *value added services*.

SECOND PASS: (10) vendors were eliminated who scored less than 90%. A few of the vendors scored reasonably well on *company capabilities, qualifications and implementation methodologies*. Nevertheless we had to consider their *company capabilities* for future the planned Managed Security Services, in terms of scale and scope, therefore they did not advance to the final pass.

THIRD PASS: (5) vendors scored more than 90% reached to the final pass. Among them, the top (3) vendors were identified as follows:

- Data Defenders (1st)
- Crowe LLP (2nd)
- Sentinel (2nd)
- Wave Solutions (3rd)

Both Crowe and Sentinel scored 94% and ranked second in the final pass. Both these vendors have equal scoring. Their capabilities, qualifications, services and implementation methodologies are very competent.

Both Crowe and Sentinel have provided professional services to the City of Aurora for years therefore portfolio diversity is required to view security from a different perspective.

Wave Solutions scored 93% and ranked in the third and final pass. Although Wave Solutions is an Aurora based company their cyber security practice is at early stages of development and lacks a proven track record.

Data Defenders was identified and selected as the top scorer with 96%. Their partnership with CA Technologies – Broadcom Company provides the perfect depth and breadth of enterprise security software—from application security testing, API security, identity and access management and privileged access management to fraud and risk detection and prevention—helps protect 49 of the Fortune 50 organizations in the world and provides the ability to propel the City of Aurora forward into the new digital world.

Funding for this purchase comes from 2019 DP – Cyber Security & Managed Services; Account 101-1380-419.32-80; not to exceed the budget amount of $140,000.