**File #:** 19-0914, **Version:** 1

**TO:** Mayor Richard C. Irvin

**FROM:** Michael R. Pegues, Chief Information Officer
Leela Karumuri, Manager IT Risk & Compliance

**DATE:** October 7, 2019

**SUBJECT:**
Request for Approval for Project Change Orders to Append Approved resolution 19-175 dated June 11, 2019 for IT Risk Assessment by Data Defenders in an amount not to exceed $54,000.

**PURPOSE:**
Due to the increase in current threat activities and ransomware attacks against municipalities around the country and the major financial losses incurred (i.e. Atlanta, Baltimore, etc.), the City's Cybersecurity team is recommending additional external penetration testing and an extension of the Incident Response Plan that was initially approved by council.

This objective will strengthen and increase the level of security and protective countermeasures for our information systems and critical infrastructure used within the City of Aurora government.

**BACKGROUND:**
This CHANGE ORDER #1 - EXTERNAL PENETRATION TESTING

Definition: External penetration testing is a practice that assesses the externally facing assets for an organization. During an external penetration test, the assessor attempts to enter the internal network by leveraging vulnerabilities discovered on the external assets.

Data Defenders per industry standards will conduct the necessary penetration testing to develop its final report and out-briefs.

External Network Penetration Testing Scope of Work (SOW) will include the following tasks:

Intelligence Gathering:

The information-gathering phase of network penetration testing methodology consists of service enumeration, network mapping, banner reconnaissance and more. Host and service discovery efforts results in a compiled list of all accessible systems and their respective services with the goal of obtaining as much information about the systems as possible.

Host and service discovery includes initial domain foot printing, live host detection, service

enumeration and operating system and application fingerprinting. The purpose of this step is to collectively map the in-scope environment and prepare for threat identification.

Threat Modeling:

With the information collected from the previous step, security testing transitions to identifying vulnerabilities within systems. This begins with automated scans initially but quickly develops into deep-dive manual testing techniques. During the threat-modeling step, assets are identified and categorized into threat categories. These may involve sensitive documents, trade secrets, financial information but more commonly consist of technical information found during the previous phase.

Vulnerability Analysis:

The vulnerability analysis phase involves the documenting and analysis of vulnerabilities discovered because of the previous network pen testing steps. This includes the analysis of out from the various security tools and manual testing techniques. At this point, a list of attractive vulnerabilities, suspicious services and items worth researching further has been created and weighted for further analysis. The plan of attack is developed here.

Exploitation:

Unlike a vulnerability assessment, a network penetration test takes such a test quite a bit further specifically by way of exploitation. Exploitation involves carrying out the vulnerability's exploit (i.e., buffer overflow) to be certain if the vulnerability is truly exploitable. During a network penetration test, this phase consists of employing heavy manual testing tactics and is often quite time-intensive. Exploitation may include, but is not limited to: buffer overflow, SQL injection, OS commanding and more.

Reporting:

The reporting step is intended to deliver, rank and prioritize findings and generate a clear and actionable report, complete with evidence, to the project stakeholders. The presentation of findings can occur via WebEx or in-person - whichever format is most conducive for communicating results. We consider this phase to be the most important and we take great care to ensure we've communicated the value of our service and findings thoroughly.

The scope of change will include the following:

1. More details on the External Penetration Testing tasks are outlined in the SOW section (see attached CHANGE ORDER 001 | 20180213-01.pdf)

2. The total change request cost is $36,000.00.

CHANGE ORDER #2 - INCIDENT RESPONSE PLAN DEVELOPMENT

Definition: An Incident Response Plan is a systematic and documented method of approaching and

managing situations resulting from IT security incidents or breaches. It is used in enterprise IT environments and facilities to identify, respond, limit and counteract security incidents as they occur.

Additional scope for the Incident Response Plan enhancement will include the following:

Business Impact Analysis:

Data Defenders will work with the COA CIO and Incident Response Team (IRT) to conduct a business impact analysis to document the areas of greatest concern in the infrastructure. The results will be used to help
prioritization of incidents during triage for incident response and to develop the necessary workflows based on the related categorizations.

Incident Categorization and Response Workflows:

Data Defenders will work with the COA IRT to identify the top reportable events and incidents about which the City is concerned and work with the team to develop and document dedicated response workflows and escalation procedures for each concern.

Assessment Methodology:

Data Defenders will work with the COA IRT to develop an assessment methodology to determine the priority of an incident relative to other incidents identified in the environment based on the type, source, and target of the incident (target mapped to BIA results).

Incident Response Tabletop Exercise:

Data Defenders will develop and facilitate an Incident Response tabletop exercise to test the COA IRT and key stakeholders on their ability to execute response capabilities for the highest priority concerns for the City.

The scope of change will include the following:

More details on the Incident Response Plan tasks are outlined in the SOW section (see attached CHANGE ORDER 002 | 20190212-01-001-02.pdf)

2. The total change request cost is $18,000.00.

**DISCUSSION:**
The expanded scope of these tasks will not change the overall timeline of the project as the additional tasks will be performed in parallel with the current SOW timeline. Project related information has been previously provided to Data Defenders and in the areas that will be included in the expanded scope of work, we can take advantage of some cost and time saving opportunities.

The Overall Summarized Cost (to date) are as follows:

Original Total Project Cost (Pre-Change) $86,000.00

| | |
|---|---|
| External Penetration Testing (Additional Scope) | $36,000.00 |
| Incident Response Plan Development (Additional Scope) | $18,000.00 |
| Subtotal (Additional Scope) | $54,000.00 |
| DP Budgeted Amount (Post-Change) | $140,000.00 |

Total funding of $54,000.00 for the change orders will be charged to account 101-1383-419.32-80 with a remaining balance of $101,000.

**IMPACT STATEMENT:**
Considering existing cybersecurity threats, the City of Aurora is responsible for warehousing and protecting an extensive volume of sensitive data. As such, implementing this comprehensive citywide security-focused Incident Response Plan is paramount to the City's cybersecurity efforts.

**RECOMMENDATIONS:**
Recommend approval for Project Change Orders: External Penetration Testing and Incident Response Management Plan from Data Defenders, 10W. 35th St, Suite 9F-5-1, Chicago, Illinois. The total amount not to exceed $54,000.00.

cc: Finance Committee

CITY OF AURORA, ILLINOIS

RESOLUTION NO. _____
DATE OF PASSAGE _____

A Resolution Approving the Request for Project Change Orders to Append Approved resolution 19-175 dated June 11, 2019 for IT Risk Assessment by Data Defenders in an amount not to exceed $54,000.

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, as part of the City of Aurora Technology Strategic Plan or “IT Roadmap” for 2019, the Information Technology Division was seeking to evaluate and improve Governance and Security citywide; and

WHEREAS, due to the increase in current threat activities and ransomware attacks against municipalities around the country and the major financial losses incurred (i.e. Atlanta, Baltimore, etc.),

the Cybersecurity team decided the City was in need of additional external penetration testing and an extension of the Incident Response Plan that was initially approved by council; and

WHEREAS, considering the threat of malicious outsiders and hackers, the City of Aurora is responsible for maintaining and protecting sensitive data; and

WHEREAS, this objective will strengthen the level of security and protective countermeasures for our information systems and critical infrastructure used within the City of Aurora government; and

WHEREAS, funding for this purchase comes from account 101-1383-419.32-80; with a budgeted amount of $101,000

NOW, THEREFORE, BE IT RESOLVED by the City Council of the City of Aurora, Illinois, as follows: Recommend the approval for Project Change Orders to append the approved resolution 19-175 dated June 11, 2019 for IT Risk Assessment with the addition of External Penetration Testing and extension of Incident Response Plan from Data Defenders, 10W. 35th St, Suite 9F-5-1, Chicago, Illinois. The total amount not to exceed $54,000.00.