File #: 20-0218, **Version:** 1

TO: Mayor Richard C. Irvin

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

DATE: March 16, 2020

SUBJECT:
Request approval for contract amendment on approved Resolution 19-175 dated June 11, 2019 for IT Risk Assessment, Data Defenders, LLC. Corporate Headquarters: 111 W. Jackson Blvd., Suite 1700 Chicago, IL 60604 in the amount not to exceed $137,550.00.

PURPOSE:
Threat activities against local municipalities have significantly escalated over the past month causing municipalities such as New Orleans, LA. and Pensacola FL. to report major cybersecurity and ransomware attacks against their technology infrastructures and business operations. Additionally, threat activities from state-based actors against U.S. based targets have significantly increased as well, evidenced by traffic from unknown IP addresses originating from countries like Iran to the City of Aurora's technology infrastructure. Most recently, the coronavirus disease: COVID-19 outbreak was declared a Public Health Emergency of International Concern on 30 January 2020.

Recognizing the increased level of potentially malicious activity against City of Aurora technology infrastructure, business continuity and disaster recovery planning has generated concerns by executive management and municipal leaders that potentially malicious threat sources are conducting reconnaissance activities and affecting threats against city infrastructure. This recognition has translated into the need to prioritize and accelerate efforts to develop and implement the necessary cybersecurity related processes and procedures, reduce the risk footprint and position the city to appropriately and effectively handle cyber-related incidents.

The City's Cybersecurity Team is recommending additional Internal Network Penetration Testing, Web Application Testing and a Disaster Recovery Plan. The objective will strengthen and increase the level of security and protective countermeasures for information systems and critical infrastructure used within the City of Aurora government.

BACKGROUND:
AMMENDMENT SECTION # 3 - DISASTER RECOVERY PLAN DEVELOPMENT

Definition: A Disaster Recovery Plan (DRP) is a business plan that describes how work can be resumed quickly and effectively after a disaster. Disaster recovery planning is just part of business continuity Planning and applied to aspects of an organization that rely on an IT infrastructure to

function.
The purpose of the disaster recovery plan for the City of Aurora is to create a set of documented processes and/or procedures to execute the municipality's disaster recovery processes to protect the city's IT infrastructure in the event of a disaster. It is a comprehensive statement of consistent actions to be taken before, during, and after a disaster.

The primary objective of disaster recovery planning is to enable the municipality to survive a disaster and to continue normal business operations while minimizing disruption as a result of the incident that impacts normal operations. In order to survive, the city must assure that critical operations can resume/continue normal processing.

The primary benefits of the City of Aurora's disaster recovery (DR) plan are as outlined:

The DR plan will minimize system and business process disruption that may occur resulting from a related incident.

The DR plan minimizes potential financial impact and losses due to system and business process disruption.

The DR plan will minimize the potential impact of threats to vulnerabilities within the city's infrastructure.

The DR plan helps to establish and enhance the foundational confidence to pursue advancement of best practices, business operations, and Smart Cities strategy.

Additional critical contingency planning components are the integration of their crisis management process, emergency notification system and incident response process

More details on the Disaster Recovery plan are outlined in the SOW section (see attached)

2. The total amendment cost is $53,250.00.

AMMENDMENT SECTION # 4 - INTERNAL NETWORK PENETRATION AND WEB APPLICATION TESTING

Definition: An Internal Network Penetration Test mimics the actions of an actual attacker exploiting weaknesses in network security without the usual dangers. This test examines internal IT systems for any weakness that could be used to disrupt the confidentiality, availability or integrity of the network, thereby allowing the organization to address each weakness.

Definition: Web application penetration testing is the process of using penetration testing techniques on a web application to detect its vulnerabilities. It is similar to a penetration test and aims to break into the web application using any penetration attacks or threats.

Phase 2 of the vulnerability management effort is to conduct both an internal network penetration test as well as a web application penetration test on targeted COA internal network components and web

application assets. The purpose of internal network penetration testing is to conduct a deeper, more manual and comprehensive assessment of COA's network infrastructure. Internal Penetration Testing is the next phase of vulnerability management and will allow Data Defenders' network penetration testers to manually assess targeted networks by conducting the same tasks of:

Foot Printing/Discovery
Enumerations
Vulnerability Analysis
Exploitation

As would be conducted by a true malicious attacker. This second phase of vulnerability assessment can identify and validate specific attack vectors that a malicious attacker would seek to exploit within the internal network infrastructure with the objective of escalating privileges to compromise information assets and resources. Internal Penetration Testing will enable issue identification, prioritization and remediation that could not be identified during the internal network vulnerability assessment.

The purpose the web application penetration testing is to identify application layer vulnerabilities within critical applications that a malicious attacker could exploit from an external perspective. Web Application Penetration Testing involves both authenticated (per user role) and unauthenticated based testing with the objectives of identifying vulnerabilities and other potential issues that would not be discovered during a typical external penetration test. This assessment focuses on testing all web application functionality available to authorized users and users with no credentials to the application (s).

The benefits of conducting internal network and web application penetration testing are as follows:

Internal Network Penetration Testing Benefits

Aids in identifying and mitigating highly probable internal threats by identifying potential attack vectors.

Validates the effectiveness of current network security countermeasures, network segmentation, and incident response capabilities to mitigate active and persistent threats to COA's technology infrastructure. Enables the fine-tuning of these countermeasures to improve their effectiveness to protect the technology infrastructure and mitigate active and persistent threats.

Validates and enables the defense-in-depth strategy by testing, validating, and improving internal security controls.

Targeted Web Application Penetration Testing Benefits

Identify the vulnerabilities that could lead to compromised applications and data breaches provides the foresight needed to strengthen your web applications and keep the most sensitive assets secure.

An experienced tester will take time to learn and understand the context of the application. Many of the vulnerabilities are simply not picked up by automated tools.

More details on the Internal and Web Application Penetration Testing tasks are outlined in the SOW section (see attached)

The total amendment cost is $84,300.00.

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-Amendment)	$140,000.00
Internal & Web Pen Testing (Amendment #4)	$ 84,300.00
Disaster Recovery Plan (Amendment #3)	$53,250.00 Subtotal
(Additional Scope)	$137,550.00
Budgeted Amount (Post-Amendment)	$277,550.00

Total funding of $137,550.00 for the amendment will be charged to account 101-1383-419.32-80 that has a 2020 budget in the amount of $534,000.00.

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 Disaster Recovery Plan, Internal Penetration testing and Web Application Testing is paramount to the City's cybersecurity efforts for proactive IT risk management.

RECOMMENDATIONS:
Recommend approval for amendments: Disaster Recovery Plan, Internal Penetration testing and Web Application Testing from Data Defenders, LLC. Corporate Headquarters: 111 W. Jackson Blvd., Suite 1700 Chicago, IL 60604. The total amount not to exceed $137,550.00.

cc: Finance Committee

CITY OF AURORA, ILLINOIS

RESOLUTION NO. _____
DATE OF PASSAGE _____

A Resolution requesting approval for contract amendment on approved Resolution 19-175 dated June 11, 2019 for IT Risk Assessment, Data Defenders, LLC. Corporate Headquarters: 111 W. Jackson Blvd., Suite 1700 Chicago, IL 60604 in the amount not to exceed $137,550.00.
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, Threat activities against local municipalities have significantly escalated over the past month causing municipalities such as New Orleans, LA. and Pensacola FL. to report major cybersecurity and ransomware attacks against their technology infrastructures and business operations. Additionally, threat activities from state-based actors against U.S. based targets have significantly increased as well, evidenced by traffic from unknown IP addresses originating from countries like Iran to the City of Aurora’s technology infrastructure; 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, the city is requesting additional services to resolutions R19-175 and R19-370; and

WHEREAS, funding for this purchase comes from account number 101-1383-419.32-80; with a 2020 budget of $534,000.00

NOW, THEREFORE, BE IT RESOLVED by the City Council of the City of Aurora, Illinois, as follows: requesting approval for contract amendment on approved Resolution 19-175 dated June 11, 2019 for IT Risk Assessment, Data Defenders, LLC. Corporate Headquarters: 111 W. Jackson Blvd., Suite 1700 Chicago, IL 60604 in the amount not to exceed $137,550.00