INFORMATION TECHNOLOGY DIVISION; CITY OF AURORA, IL

PROFESSIONAL SERVICES CHANGE ORDER

Client Contact: Michael Pegues
Contract Number: 20190213-01
Work Order Number: 001
Change Order Number: 003
Change Order Date: February 19, 2020
Engagement Manager: Cyrus Walker

Introduction

This Project Change Order Request is Appended to the Contract Services Agreement for services by and between Data Defenders and City of Aurora, IL Information Technology Division (COA) dated June 20, 2019 ("Agreement").

Schedule Number: 003 Effective Date: February 19, 2020

This Project Change Order Request is governed by the above referenced Agreement, the terms and conditions of which are hereby incorporated into this Project Change Order Request by this reference. The terms of this Project Change Order Request shall control if there is a conflict with the terms of the Agreement. The following defines the Project Change Order Request to be provided by Data Defenders.

Project Name	Cybersecurity Assessment
Requested By	City of Aurora, IL
Presented To	Michael Pegues, Chief Information Officer
Change Name	Project Scope Change
Change Number	003
Date of Request	February 19, 2020

Description of Change

The scope of change will include the following task(s):

1. **Information Technology Disaster Recovery Plan Development**

Reason for Change

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.

Recognizing the increased level of potentially malicious activity against COA's technology infrastructure has generated concerns by COA senior IT management and municipal governance that potentially malicious threat sources are conducting reconnaissance activities and affecting threats against COA's technology infrastructure. This recognition has translated into the need to prioritize and accelerate efforts to develop and implement the necessary cybersecurity related processes and procedures to mature COA's Disaster Recovery capabilities to position and enable COA to appropriately and effectively handle cyber-related incidents

Michael Pegues, CIO of COA requested the change of scope to the current Cybersecurity Assessment project being conducted by Data Defenders to expand the scope of the project to include the development and implementation of an Information technology focused Disaster Recovery plan. The addition of this task will add to the overall timeline but will not delay the completion of the current Cybersecurity Assessment currently in progress. The additional tasks will be performed in parallel with the current SOW Timeline.

Statement of Work for Change Order

STATEMENT OF WORK SUMMARY

Data Defenders is being engaged by COA to develop a new Disaster Recovery plan. The scope of work to conduct this task is outlined below.

TASK #1 –DISASTER RECOVERY PLAN DEVELOPMENT

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 COA DR plan will minimize system and business process disruption that may occur resulting from a related incident.
- The COA DR plan minimizes potential financial impact and losses due to system and business process disruption.
- The COA DR plan will minimize the potential impact of threats to vulnerabilities within the COA technology infrastructure.
- The COA DR plan helps to engender and establish the foundational confidence to pursue advancement of the COA's IT, 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.

The following table provides a high-level breakdown of the sub-tasks and estimated hours associated with each sub-task required to complete the DR plan development.

ESTIMATED HOURS ALLOCATION PER TASK TABLE		
Project Tasks/Deliverables		**Estimated Hours**
TASK #1B – Disaster Recovery Plan Development *(Create Framework for Disaster Recovery)*	Create policy document	275 Hours
	Create standards document	
	Create objectives document	
	Create metrics document	
	Create network disaster recovery plan	

ESTIMATED HOURS ALLOCATION PER TASK TABLE		
Project Tasks/Deliverables		**Estimated Hours**
	Enhance telecommunications disaster recovery plan	
	Create applications/database disaster recovery plans (i.e., each mission critical application)	
	Create server/storage disaster recovery plans	
	COOP Enhancements	
	Identify SMEs for IT Infrastructure components (i.e., network, applications, servers, database, storage)	
	Determine follow up timeline	
	Approval from key stakeholders	
TASK #1D – Disaster Recovery Plan *(Project Management)*	Project Management of DRP Development Tasks/Technical Documentation	30 Hours
DRP Contingency*	Contingency Set of Hours for DR Plan Development Tasks	50 Hours*

***The Contingency set of hours identified in the table above are allocated to cover time overages that may occur during the execution of with the DR tasks. This contingency set of hours will be used only after the direct, written approval of COA management.

Change of Project Scope Benefits

The addition of these tasks to the current project scope will position COA to reduce the risk of a cybersecurity incident negatively impacting its business operation. The following is a list of specific benefits for adding each task that COA will experience as a result of adding the additional tasks to the current project scope of work.

- **Disaster Recovery Plan Development**

  A well-developed, implemented, and tested Disaster Recovery Plan ensures that COA will be able to appropriately respond and recover IT operations and systems when a cyber or other events occur that negatively impact COA business and IT operations. Recent incidents in Baltimore and Atlanta that impacted not only system operations but also their ability to collect revenue, support property sales, manage police and public safety operations, and threatened PII managed by their HR function cost these cities approximately $37 Million and $7 million respectively in lost revenue and recovery expenditures. These incidents highlight the significant need for a well-developed, implemented, and test Business Continuity and Disaster Recovery plan which would have significantly reduces their financial losses.

A plan of this nature supports a prescribed response based on the type of incident and also streamlines the execution of a response which will enables COA to minimize the financial liability and any damage to its resident's trust that may occur as a result of the incident.

Effect on Deliverables (Including a List of Any Affected Deliverables)

The following deliverables will be added to the overall SOW:

a. IT Disaster Recovery Plan

Effect on Project Schedule (Including Estimated Completion Date for This Change)

Upon approval of this Change Order 003, Data Defenders will develop a project plan for each of the tasks outlined in this Change Order which will outline the project timelines for each task. However, the project timelines associated with these new tasks will be conducted in conjunction with the currently approved project timeline but will not affect the duration of that timeline. Data Defenders will work with COA Senior IT Management to develop the relative project plans and timelines for Task #1 –Disaster Recovery Plan Development.

Effect on Project Cost

This section provides a detailed explanation of the cost associated with the tasks defined in this Change Order. Please note the following:

Item Description	Hours		Dollars	
	Reduction	Increase	Reduction	Increase
TASK #1 – Disaster Recovery Plan Development Task				
Disaster Recovery Plan Development		275 Hours		$ 41,250.00
Project Management/Report Development		30 Hours		$ 4,500.00
DRP Contingency*		50 Hours		$ 7,500.00
Sub-Total Cost Change Order #003				**$ 53,250.00**
Original Total Project Cost (Pre-Change)				$ 140,000.00
Total Project Cost				**$ 193,250.00**

Signatures

DATA DEFENDERS ENGAGEMENT MANAGER

☒ **Approved** **Signature:** _____

☐ **Rejected** **Title:** **Managing Principal** **Date:** _____

CITY OF AURORA, IL

☐ **Approved** **Signature:** _____

☐ **Rejected** **Title:** _____ **Date:** _____

WE ARE THE DEFENDERS OF YOUR INFORMATION WORLD!

Data Defenders, LLC.
Corporate Headquarters:
111 W. Jackson Blvd., STE. 1700
Chicago, IL 60604

(WEB): www.data-defenders.com
(EMAIL): info@data-defenders.com

(MAIN): (312) 224-8831
(FAX): (312) 242-1795