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: 004
Change Order Date: February 26, 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: January 6, 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	January 6, 2020

Description of Change

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

1. **Internal Penetration Testing/Web Application Penetration Testing**

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 vulnerability management 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 a second, more intense phase of vulnerability management to focus on internal network penetration testing to support COA's cybersecurity implementation efforts. 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 execute the second phase of internal vulnerability focused on internal penetration testing. The scope of work to conduct these tasks is outlined below.

TASK #1 – INTERNAL NETWORK PENETRATION AND WEB APPLICATION TESTING

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:

- Footprinting/Discovery
- Enumerations
- Vulnerability Analysis
- and 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 COA to further prioritize remediation and discover issues 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**
  a. Aids in identifying and mitigating highly probable internal threats by identifying potential attack vectors.

  b. 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.

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

- **Targeted Web Application Penetration Testing Benefits**
  a. Identify the vulnerabilities that could lead to compromised applications and data breaches This provides the foresight needed to strengthen your web applications and keep the most sensitive assets secure.

  b. 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.

c. Web applications are designed to provide access to services and information, and testing is a critical step in ensuring the code is secure, the organization is compliant, and can trust that their data is protected.

The following table provides a high-level breakdown of the sub-tasks and estimated hours associated with each sub-task required to complete the Internal network and web application penetration test.

COA INTERNAL NETWORK AND WEB APPLICATION PENETRATION TESTING PROJECT DELIVERY TIMELINE		
ASSESSMENT TASK	**EST. HOURS ALLOCTIONS**	**NOTES AND ASSUMPTIONS**
INTERNAL NEWORK PENETRATION TESTING TASKS	**360 Hrs.**	
Project Initiation		
Establish/confirm scope		
Discovery / Recon/ Enumeration (Per Network)		
Vulnerability Scanning and Manual Verification		
Initial Exploitation		
Post-Exploitation		
Report Development (Per Report)		
Post Test Activities (Remediation Confirmation)		
WEB APPLICATION PENETRATION TESTING TASKS	**190 Hours**	Up to 3 Web Applications will be targeted for the test
Application Mapping and Enumeration		
Vulnerability Scanning and Manual Verification		
Initial Exploitation		
Post-Exploitation		
Report Development (Per Report)		
Post Test Activities (Remediation Confirmation)		
PROJECT MANAGEMENT TASKS		
Project Management	**12 Hours**	

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.

- **Internal Network/Web Application Penetration Testing**
  Conducting this second phase of vulnerability management enables COA to conduct a deeper identification and verification of vulnerabilities that could be exploited by a malicious attacker. This

level of vulnerability identification gives COA the ability to continue to mitigate the risk of a cybersecurity breach.

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

The following deliverables will be added to the overall SOW:

a. Internal Network Penetration Testing Results Report

b. Web Application Penetration Testing Results Report

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 this new task 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 Internal Network/Web Application Penetration Testing.

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:

- ### Task #1 – Internal Network/Web Application Penetration Testing Cost Estimates

  Data Defenders is providing an allocation of hours to be used by COA for Internal Network and Web Application Penetration Testing activities. Time accrued for execution of activities associated with this task will be billed to COA on hourly basis. COA will be responsible for defining the target devices and target web applications for internal penetration and web application penetration testing. The allocation of hours for this task are highlighted in the following table.

Item Description	Hours		Dollars	
	Reduction	Increase	Reduction	Increase
TASK #1 – Internal Network/Web Application Penetration Testing				
Internal Network Penetration Testing		360 Hours		$ 54,000.00
Web Application Penetration Testing		190 Hours		$ 28,500.00
Project Management/Report Development		12 Hours		$ 1,800.00
Sub-Total Cost Change Order #004				**$ 84,300.00**
Original Total Project Cost (Pre-Change – Includes Cost for Change Order #003)				$ 193,250.00
Total Project Cost				**$ 277,550.00**

Signatures

DATA DEFENDERS ENGAGEMENT MANAGER

☒ **Approved** **Signature:** _____

☐ **Rejected** **Title:** _____ **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