DATA DEFENDERS
Defenders of the Information World™

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 Date: July 31, 2019
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: 001 Effective Date: September 1, 2019

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	External Penetration Testing
Requested By	City of Aurora, IL
Presented To	Michael Pegues, Chief Information Officer
Change Name	Project Scope Change
Change Number	001
Date of Request	July 28, 2019

Description of Change

The scope of change will include the following:

1. Addition of an External Penetration Testing task as outlined in the SOW section.
2. The pricing of the overall project will increase from the current price of $86,000.00 to $122,000.00.

Reason for Change

Michael Pegues, CIO of COA requested the addition of the External Penetration Testing task to the Cybersecurity Assessment Scope of Work. The addition of this task will not change the overall timeline of delivery as the additional task will be performed in parallel with the current SOW Timeline.

Statement of Work

STATEMENT OF WORK SUMMARY

Data Defenders is being engaged by COA to perform External Penetration Testing services. The scope of work to conduct an external network penetration testing for the City of Aurora is provided below and according the IPs/URLs that were previously submitted to Data Defenders by COA IT Management.

TASK #1 – EXTERNAL PENETRATION TESTING

Data Defenders projects that penetration testing for estimated 160 externally facing IPs/URLs will take approximately 20 days to complete with an additional 10 days to develop the final report and out-briefs.

External Network Penetration Testing Scope of Work 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 as a result 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. In essence, 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 actually carrying out the vulnerability's exploit (ie: buffer overflow) in an effort 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.

- **Penetration Testing Scope Determination**

  a. Develop Rules of Engagement document.

  b. Determine External IP ranges *(External IP ranges will be defined in the Rules of Engagement document)*

  c. Authenticated/Unauthenticated

  d. Collect public, readily available internal/external information or no IT environment Context for conducting test.

  e. Determine Social Engineering Component.

  f. Determine setup and penetration vantage point - External/DMZ/Internal initial scans/with or without WAF

  g. Define SIRT Awareness level/Monitoring testing

- **Preliminary Set up of Penetration Test.**
  a. Confirm Client Tasks Completed for setup
  b. Level One Scans - Authenticated or Unauthenticated/Restrictions for timing of scans/Invasive or Evasive in nature
  c. Discovery and Reconnaissance- Assets, Ingress/Egress Ports, Threats Vulnerabilities.
  d. Configuration of Penetration Testing Tool Suite (Perimeter, Internal based on IP Ranges, and Desired level of device configuration, system components, DMZ, web tier, data tier, application and infrastructure tiers based on client scope).
  e. Scheduling Penetration test and Notification of Testing Alert, if required

- **Penetration Testing**
  a. Conduct Penetration test/Collect Data Samples/Validate Evidence of Vulnerability versus Ability to Exploit (determined in client Scope)
  b. Client meetings schedule to address issues, validate testing within client scope, provide status on any high severity findings requiring immediate attention, or trends in data collecting not covered in scope

- **Penetration Testing Follow-Up Tasks**
  a. Conduct any follow up testing required given scope of testing and initial findings in preliminary set-up phase.
  b. Formally discuss issues and severity with each customer's Security Engineers and IT Risk designates to validate findings.
  c. Create Draft Report/Review with Customer Sponsor/Stakeholder for feedback

- **Develop Final Customer Report**
  a. Submit final reports
  b. Two-week remediation period for retesting, if applicable

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

The following deliverables will be added to the overall SOW:

a. Rules of Engagement

b. External Penetration Testing Final Report

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

Data Defenders will engage project resources to execute the above work in parallel to current work-streams. The overall project delivery and timeline objectives will not change as a result of the addition of this task.

Effect on Project Cost

Item Description	Hours		Dollars	
	Reduction	Increase	Reduction	Increase
External Penetration Testing		240 Hours		$36,000.00
Total Change Request Cost				$36,000.00
Original Total Project Cost (Pre-Change)				$86,000.00
New Total Project Cost (Post-Change)				$122,000.00

Signatures

DATA DEFENDERS ENGAGEMENT MANAGER

☒ **Approved** **Signature:** ______________________________

☐ **Rejected** **Title:** **Managing Principal** **Date:** **7/31/2019**

CITY OF AURORA, IL

☐ **Approved** **Signature:** ______________________________

☐ **Rejected** **Title:** ______________________ **Date:** ______________

WE ARE THE DEFENDERS OF YOUR INFORMATION WORLD!

Data Defenders, LLC.
Corporate Headquarters:
University Technology Park at IIT
10 W. 35th St. Suite 9F5-1
Chicago, IL 60616

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

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