INFRASTRUCTURE & TECHNOLOGY COMMITTEE UPDATE

Resolution 21-0311

Executive Summary

Resolution 21-0311 : Amend approved **Total amount not to exceed $3,202,215 over the five-yea** resolution R20-311, dated December 22, 2020, (Legistar item 20-0815) from Data Defenders LLC, 111 Jackson Blvd, Suite 1700, Chicago IL 60604 for $1,601,730. **r contract.**

Purpose: The City of Aurora, Information Technology (IT) Division is seeking to expand the scope of managed security services to include the City of Aurora **Operational Technology (OT) and Supervisory Control and Data Acquisition (SCADA) infrastructure.**

Water Treatment Facility Cyberattack Suggests More to Come

An attacker remotely accessed a Florida water treatment facility via a low-grade security system, and it's likely that others will see how easy it was and commit more cyberattacks on the nation's critical infrastructure.

February 19, 2021 • Jim McKay

The Bruce T. Haddock Water Treatment Plant, located at 350 Commerce Boulevard in Oldsmar, Fla. Local and federal authorities are investigating after an attempt Friday to poison the city of Oldsmar's water supply. Pinellas County Sheriff Bob Gualtieri said Feb. 8

The problem is that the software wasn't designed to protect critical infrastructure and probably was of residential grade, according to Randy Watkins, chief technology officer for Managed Detection and Response at cybersecurity firm CriticalStart.

"There are a couple of things that trouble me about this," Watkins said. "One is I don't think this is the only water treatment facility that's set up in this manner, and I don't think it's the only critical infrastructure that's set up in this manner."

Background: Service Additions

Goal # 1: *Implementing a Cybersecurity Program, Operation, and Technical Infrastructure of the City's OT Infrastructure which will include the following components:*

1. eSentire esNetwork Managed Detection and Response Service.
2. esEndpoint Detection and Response Powered by CrowdStrike Services.
3. Sentinel SEIM Management (includes Security Device Management or 3 devices).
4. Vulnerability Management

Goal# 2: *Adding the following Professional Services Tasks:*

1. Risk Assessment
2. Internal/External Penetration Testing.
3. vCISO Professional Services
4. Threat Intelligence Analysis (Incident Response)

Goal # 3: *Implementing Okta End-to-End Identity Management Point Solution.*

1. Single Sign on, Multi-Factor Authentication, Lifecycle Management, Universal Directory, API 2. Access Management.
3. Training- Okta Essentials
4. Okta Support-Premier Success Package
5. Design & Integration Services
6. Platform Management

Financials

Amended Scope Itemization for OT/SCADA Security:

• Service #1 Data Shield Managed Security Services (9 Mo. In 2021)		
• eSentire esNetwork Managed Detection and Response Service	2021	$44,494.00
• Service #2 Data Shield Managed Security Services		
• esEndpoint Detection & Response by CrowdStrike Services	2021	$15,833.00
• (9 Mo. In 2021)		
• Service #3 Price Level: Fixed Price SEIM/Security Device	2021	$14,700.00
• Service #4 Price Level: Fixed Price Vulnerability (9 Mo. In 2021)	2021	$11,250.00
• Service# 5 Data shield Professional Services		
Risk Assessment	2021	$7,500.00
Internal/External Penetration Testing	2021	$7,500.00
Subtotal		**$101,277.00**

Amended Scope Itemization for IT Security:

• Service#5 Data Shield Professional Services		
Annual General hours Allocation	2021	$11,250.00
VCISO	2021	$37,500.00
Threat Intelligence Analysis	2021	$45,000.00
• Service#6 Data Shield Point Solutions	2021	$79,352.00
(Okta Identity Management)(Partial 9 Mo. In 2021)		
• Policy Development	2021	$20,250.00
(15 different subject matters and 5 potential Policies)		
• Design & Integration Services (One-Time Costs)	2021	$30,000.00
• Training – Okta Essentials (One-Time Costs)	2021	$ 3,149.00
Subtotal		**$218,750.00**
Total amount annually for both OT/SCADA & IT	2021	**$327,778.00**

Financials continued

Contract Amendment Summary

Budget Year	Amount
2021	$327,778.00
2022	$318,488.00
2023	$318,488.00
Optional Years	
2024	$318,488.00
2025	$318,488.00

Budget

- The IT budget has sufficient funds to cover the first year of this contract as Cyber spending was budgeted in 101-1383-419.32-80 at $757,600.00. While the total expenses associated with the Water Fund total to $101,277.00, there is not sufficient funds budgeted in the Water fund to cover this expense. Water Fund account # 510-1380-511.32-20 Contracted Services had $80,000 budgeted in 2020 but this was cut in 2021 as a part of the 5% decrement requirement. Account 510-1380-511.64-10 Software Applications has a budget in 2021 of $52,000 of which $31,040 will be allocated to this Cyber SCADA service cost. Taking this into account:
  - Partial funding available in IT account # 101-1383-419.32-80 Professional Fees/Consulting Fees $296,738
  - Partial funding available in Water Fund account # 510-1380-511.64-10 Software Applications $31,040.00.

- Water Fund expenses will need to be increased beginning in 2022 to cover this new expense, however this could also result in a decrease to the General Fund portion of the Cyber contract costs by same amount, reducing that budget by an equal amount in the IT budget. The Budget Team and Public Works/Water team (with IT input in those areas) will be reviewing the total support provided by the Water Fund to the General Fund for all administration, IT, and other services in the 2022 budget process as this new expense represents a significant enough increase to re-examine that interfund relationship.

- While this total expense appears to be a major increase to IT expenses, the current IT budget is above $10 million when all departments are considered and as such, this expense equates to 6% of total IT expenses over 5 years. This investment is prudent to reduce risk, maintain operational and business continuity in the cyber domain

Thank you

According to Gartner, the recommended annual Cybersecurity spend is **$855k**.

Recommended IT Security Spend for State/Local Government*	
Recommended Annual IT Security Spend based on Total Annual IT Spend	$ 600,000.00
COA Annual IT Spend	$15,000,000.00
COA Current Annual IT Security (2021)	$360,000
Recommended Annual IT Security Spend	$855,000.00
COA Annual IT Security Spend Variance	-$495,000 (54%)

* Reference: Gartner IT Key Metrics Data 2020: IT Security Measures - Analysis

Data Shield's annual comparative cost for a similar in-house service footprint is more than 85% less than the annual cost to build, staff, and managed daily in-house SOC operations network devices, monitoring, response, and reporting services

In-House SOC Staffing Model

Function	Required FTEs	Annual Salary	Total Annual Cost
Threat Detection & Response	4	$ 150,000.00	$ 600,000.00
Vulnerability Management	2	$130,000.00	$ 260,000.00
Cybersecurity Assessment	2	$ 120,000.00	$ 240,000.00
NIST RMF	1	$ 135,000.00	$ 135,000.00
Disaster Recovery	1	$ 140,000.00	$ 140,000.00
Penetration Testing	2	$ 145,000.00	$ 290,000.00
Compliance Auditor	1	$ 145,000.00	$ 145,000.00
		Total In-House SOC Annual Cost*:	**$ 1,810,000.00***

*Staffing Only Costs. Does not include the annual capital cost of required to support in-house SOC operations, staff benefits, etc.

Source: **Gartner IT Key Metrics Data 2020: IT Security Measures** — Analysis Published: 18 December 2019
ID: G00465697