Headquarters
18480 Bandilier Circle
Fountain Valley, CA 92708
(714) 593-7433

File #: 2025-4582 **Agenda Date:** 11/12/2025 **Agenda Item No:** 6.

FROM: Robert Thompson, General Manager
Originator: Wally Ritchie, Director of Finance

SUBJECT:

INDUSTRIAL CONTROL SYSTEM PENETRATION TEST AND VULNERABILITY ASSESSMENT

GENERAL MANAGER'S RECOMMENDATION

RECOMMENDATION:

A. Approve a Purchase Order Contract to Carahsoft Technology Corp for the purchase of an Industrial Control System Network Penetration Test and Vulnerability Assessment utilizing the cooperative OMNIA Software Solutions and Services Contract No. R240303, for a total amount not to exceed $210,750 (Includes Sales Tax); and

B. Approve a contingency in the amount of $21,075 (10%).

BACKGROUND

Orange County Sanitation District (OC San) is upgrading the existing Supervisory Control and Data Acquisition (SCADA) Systems for the treatment plants and pump stations as part of Project J-120 Process Control Systems Upgrades. The project will replace existing obsolete human-machine-interface systems, databases and software programs including trending, diagnostic data, monitoring, control, alarming and reporting.

RELEVANT STANDARDS

- Protect OC San assets
- Ensure the public's money is wisely spent
- 24/7/365 treatment plant reliability
- Maintain a culture of improving efficiency to reduce the cost to provide the current service level or standard

PROBLEM

When new systems and applications are introduced, they can bring about various vulnerabilities and risks. This is primarily because these new technologies may not have been thoroughly tested in all possible scenarios, leading to unforeseen security gaps. They may also include unpatched or vulnerable third-party components, suffer from configuration errors or weak access controls, and create new integration points that expose data or systems to attack.

PROPOSED SOLUTION

An Industrial Control System (ICS) Network Penetration Test and Vulnerability Assessment can identify system and application vulnerabilities and weaknesses.

An ICS Network Penetration Test is designed to determine susceptibility to an actual attack by trying to infiltrate the target environment using current, real-world tactics, techniques and procedures. Findings and recommendations are identified and are prioritized based on the potential for process or system disruption.

An ICS Network Vulnerability Assessment is designed to identify vulnerabilities in industrial networks and prioritize recommendations based on potential system impact. These include known software vulnerabilities, weak security controls, misconfigurations, and other system weaknesses.

TIMING CONCERNS

It is crucial to identify vulnerabilities and weaknesses and mitigate them as soon as possible. If the adversaries were to find and exploit them, they could possibly gain access and perform malicious activities.

RAMIFICATIONS OF NOT TAKING ACTION

Not finding and identifying vulnerabilities or weaknesses can increase risk to these vulnerabilities being exploited by those with malintent which can result in malware infections, system failures, and system outages halting operations.

PRIOR COMMITTEE/BOARD ACTIONS

N/A

ADDITIONAL INFORMATION

Based on security review, staff recommends approving the Purchase Order Contract to Carahsoft Technology Corp utilizing the cooperative OMNIA Software Solutions and Services Contract, Contract No. R240303.

CEQA

N/A

FINANCIAL CONSIDERATIONS

This request complies with authority levels of OC San's Purchasing Ordinance. This item has been budgeted (Budget FY 2025-26 Section 8, Page 10, Treatment System Improvement Project No. J-120) and the budget is sufficient for the recommended action.

ATTACHMENT

The following attachment(s) may be viewed on-line at the OC San website (www.ocsan.gov) with the complete agenda package:

N/A