



- **Board of Directors**
Engineering, Operations, and Technology Committee

8/20/2024 Board Meeting

7-6

Subject

Authorize a \$875,000 increase to an existing agreement with Computer Aid Incorporated to a new not-to-exceed amount of \$2,625,000 for staff augmentation support services for the operation and maintenance of the Metropolitan Cybersecurity Operations Center for an additional six months; the General Manager has determined that the proposed action is exempt or otherwise not subject to CEQA

Executive Summary

This action authorizes an amendment to the agreement for operation and maintenance of Metropolitan's enterprise-wide Cybersecurity Operations Center (CSOC) to extend the termination date of the original agreement from September 30, 2024, to March 1, 2025, and increases the total value of the contract from \$1,750,000 to \$2,625,000. The purpose of this contract amendment is to ensure Metropolitan maintains cybersecurity threat monitoring capability while Metropolitan continues vendor selection and negotiates the award of the long-term Cybersecurity Operations Center-managed services contract from RFP-DH-1367. Metropolitan safeguards its information and operational technology infrastructure through a combination of cybersecurity services, monitoring, anti-malware technologies, next-generation firewalls, enhanced zero trust access control, and employee awareness education. The electronic security system integrates data from access control, intrusion detection, and video monitoring. The CSOC functions 24 hours per day, seven days per week, 365 days per year to detect, identify, contain, and remediate cybersecurity threats to Metropolitan's computers, data, and industrial control systems used to store, treat and deliver water.

Proposed Action(s)/Recommendation(s) and Options

Staff Recommendation: Option #1

Option #1

Authorize a \$875,000 increase to an existing agreement with Computer Aid Incorporated to a new not-to-exceed amount of \$2,625,000 for staff augmentation support services for the operation and maintenance of the Metropolitan Cybersecurity Operations Center for an additional six months.

Fiscal Impact: Expenditures of \$875,000 in Operations and Maintenance funds

Business Analysis: This option will implement security recommendations made by internal staff and the Department of Homeland Security and address cyber threats affecting business computer systems and Supervisory Control and Data Acquisition (SCADA) systems. This all-inclusive approach comprehensively strengthen Metropolitan's cyber security resilience.

Option #2

Do not proceed with this project at this time

Fiscal Impact: No additional expenditures of Operations and Maintenance funds

Business Analysis: This option would allow the Computer Aid Incorporated (CAI) agreement to expire and place the Cybersecurity Operations Center into a state where it could not be operationally maintained until a consultant is awarded a contract from RFP-DH-1367.

Alternatives Considered

Not applicable

Applicable Policy

Metropolitan Water District Administrative Code Section 5108: Appropriations

Metropolitan Water District Administrative Code Section 8121: General Authority of the General Manager to Enter Contracts

Metropolitan Water District Administrative Code Section 11104: Delegation of Responsibilities

Related Board Action(s)/Future Action(s)

By Minute Item 53354, dated August 15, 2023, the Board authorized the agreement with Computer Aid Incorporated in an amount not to exceed \$1,750,000.

California Environmental Quality Act (CEQA)

CEQA determination for Option #1:

The proposed action is not defined as a project under CEQA because it will not result in either a direct physical change in the environment, or a reasonably foreseeable indirect physical change in the environment. (State CEQA Guidelines Section 15378(a)). In addition, the proposed action is not defined as a project under CEQA because it involves organizational, maintenance, or administrative activities; personnel-related actions; and/or general policy and procedure making that will not result in direct or indirect physical changes in the environment. (Public Resources Code Section 21065; State CEQA Guidelines Section 15378(b)(2) and (5)).

CEQA determination for Option #2:

None required

Details and Background

Background

In August 2023, the Board authorized an agreement with CAI. This action will allow CAI to continue to centrally monitor, detect, analyze, mitigate, and respond to cyber threats on the Metropolitan Enterprise Information Technology and SCADA systems until a new contract is awarded. Metropolitan released a request for proposals (RFP) in October of 2022 for CSOC Co-Managed Services. The main purpose of the CSOC-co-managed support services is to improve real-time situational awareness resulting in Metropolitan's improved capabilities to detect, identify and respond to cyber threats. A secondary function of the CSOC is to provide critical intelligence information to Metropolitan's member agencies to enhance the overall cybersecurity posture for Metropolitan's service area.

After going through the selection process, no contract was awarded. One vendor was selected, but the final scope of work deviated too far from the original scope of work that was detailed in the RFP resulting in a cancellation of the RFP with a re-release of the RFP planned pending a more stringent re-write of the scope requirements. The result of this action is to maintain the current contract for staff augmentation support to provide Metropolitan with the minimum ability to continuously monitor for cyber threats while the RFP process is conducted.

The CSOC project was executed under the Capital Investment Plan (CIP). The CIP covered the procurement and implementation of the required technologies and the actual construction of the CSOC facility. CIP funding is not available for the co-managed services agreement. Funds for this action are available within Metropolitan's IT Group, Operations and Maintenance budget.

Objective

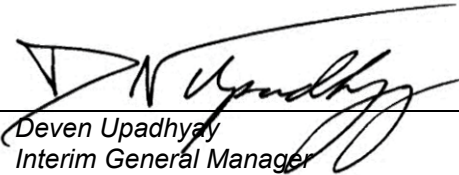
CAI would be required to continue to provide staff support for around-the-clock monitoring of CSOC systems to afford Metropolitan employees assigned to the CSOC to be free to conduct the CSOC defensive posture support such as approving cybersecurity exception requests, conduct information systems and operational technology design and upgrade support, and to conduct vulnerability scanning management activities. CAI will assist with CSOC core functions. These core functions include network monitoring and security event analysis, email security monitoring and analysis, cyber incident response and management, vulnerability assessment, security engineering, cyber intelligence support, and intrusion analysis.

The CSOC provides Information Technology and Operational Technology defensive posture support and is responsible for the overall security of the Metropolitan Enterprise-wide information systems and networks. The CSOC is established in accordance with the guiding principles of security established by the National Institute of Standards and Technology, the Metropolitan Cyber Security Program Framework, and the Metropolitan Cyber Security Policy. The CSOC is chartered to prevent, detect, contain, and eradicate cyber threats through monitoring, intrusion detection, and protective security services to Metropolitan information systems, including the Metropolitan wide area networks, local area networks, security devices, servers, and workstations. The Metropolitan CSOC also conducts vulnerability assessments, analyzes cyber threats, monitors the Metropolitan email gateway, and collects information on, investigates, and reports on all confirmed or suspected cybersecurity incidents.

Project Milestones

Onboard of Co-Managed Service Vendor	September 2024
Transition from Staff Augmentation Services to Co-Managed Services	October 2024
Co-Managed services vendor fully integrated with Metropolitan CSOC and conducting cybersecurity operational support services	January 2025


 _____ 7/30/2024
 Charles Eckstrom Date
 Group Manager, Information Technology


 _____ 7/31/2024
 Deven Upadhyay Date
 Interim General Manager