



THE METROPOLITAN WATER DISTRICT
OF SOUTHERN CALIFORNIA

Board Action

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

2/11/2025 Board Meeting

REVISED 7-3

Subject

Authorize an agreement with Computer Aid, Inc. in an amount not to exceed \$~~5.756~~ million for co-managed support services for the operation and maintenance of the Metropolitan Cybersecurity Operations Center; the General Manager has determined that the proposed action is exempt or otherwise not subject to CEQA

Executive Summary

This action awards an agreement for operation and maintenance of Metropolitan's enterprise-wide Cybersecurity Operations Center (CSOC) for a three-year period beginning March 1, 2025, with options to renew for two one-year periods not to exceed five total years on the contract.

The purpose of this contract is to provide continuous cybersecurity threat monitoring, detection, and response capability. 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 anti-malware tools. 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 an agreement with Computer Aid, Inc. (CAI) in an amount not to exceed \$~~5.756~~ million for co-managed support services for the operation and maintenance of the Metropolitan Cybersecurity Operations Center.

Fiscal Impact: Expenditures of \$~~5.756~~ million in Operations and Maintenance (O&M) funds for FY 2024/2025 and 2025/2026

Business Analysis: This option will implement cybersecurity 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 will comprehensively strengthen Metropolitan's cybersecurity.

Option #2

Do not proceed with the service at this time.

Fiscal Impact: No additional expenditure of O&M funds

Business Analysis: This option would forgo an opportunity to reduce cyber threats and increase information security risks.

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 an agreement with Computer Aid in an amount not to exceed \$1,750,000 for staff augmentation support services.

By Minute Item 53749, dated August 20, 2024, the Board authorized an increase of \$875,000 to the existing agreement with Computer Aid to a new not-to-exceed amount of \$2,625,000 for staff augmentation support services.

California Environmental Quality Act (CEQA)

CEQA determination for Option #1:

The proposed action is exempt from CEQA because there is no potential for the activity in question to have a significant effect on the environment. (State CEQA Guidelines Section 15061(b)(3)).

CEQA determination for Option #2:

None required

Details and Background

Background

Each year, Metropolitan faces hundreds of thousands of attempted compromises to Metropolitan's networks. While Metropolitan's cybersecurity tools block most of these attempts, some attacks have and will continue to succeed to some degree which could result in lost staff hours, costs associated with remediation and temporarily reduced operational capacity. It is conceivable that such threats, if not detected in a timely manner, could possibly have a catastrophic impact on Metropolitan's information and water management systems.

In 2018, Metropolitan started a project to design, construct and implement the operation of a CSOC. The construction of the CSOC facility was finished in March of 2023. Work was completed on the installation and configuration of the underlying technologies needed for the CSOC to perform its functions in November 2022. Prior to the CSOC, there was no ability for Metropolitan to continuously monitor for and respond to cybersecurity threats. However, Metropolitan is not staffed to operate the CSOC, nor is it feasible to hire and retain the skill sets needed under the existing job classifications and pay scales. For the CSOC to operate at the level it was intended, a contracted managed service is required to conduct the continuous operation.

The Cybersecurity Operation Center centrally monitors, detects, analyzes, mitigates, and responds to cyber threats on the Metropolitan Enterprise Information Technology and SCADA systems. For a year and a half, Metropolitan cybersecurity staff, with assistance under a temporary staffing contract, have operated to gather and analyze information from data centers, the disaster recovery facility, workstation networks, physical security, SCADA systems, water operations systems, and field equipment. Data is also collected and analyzed from private and government agencies such as Computer Emergency Readiness Teams and Information Sharing and Analysis Centers. Correlating this data to find suspicious activity can be extremely challenging and often only occurs long after an incident happens.

Metropolitan issued a request for proposals (RFP) in February of 2024 for CSOC co-managed services to continue to meet current staffing requirements and the requirements created by increasingly more sophisticated cyber threats. This is the main purpose of the CSOC co-managed support services. Once in place, this management model will improve real-time situational awareness, resulting in Metropolitan's increased capabilities to detect, identify and respond to cyber threats. A secondary function of the CSOC will be to provide critical intelligence information to Metropolitan's member agencies to enhance the overall cybersecurity posture of Metropolitan's system.

A review panel evaluated each proposal. Based on the panel evaluation, staff initiated contract negotiations with the top respondents as authorized in the RFP. Staff was unable to reach agreeable contracting terms with the top two respondents. Metropolitan was able to reach agreeable contracting terms with CAI to perform the required services within Metropolitan's operating budget.

Approval of this contract will create a mechanism for Metropolitan to better meet the demands of a dynamically changing cyber threat landscape while ensuring there is more than adequate staffing to monitor for cyber threats on a continuous basis, reducing the risk to the security and stability of the water supply managed by Metropolitan. 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 for fiscal biennial 2024-2026.

Once in place, CAI shall perform work at the primary Metropolitan CSOC facility located in La Verne, CA. As part of the agreement, eight personnel will operate from the Metropolitan CSOC facility twenty-four hours per day, seven days per week, and 365 days per year. Metropolitan will coordinate clearance for and grant physical access by qualified and cleared personnel into the CSOC premises and facilities and other Metropolitan sites.

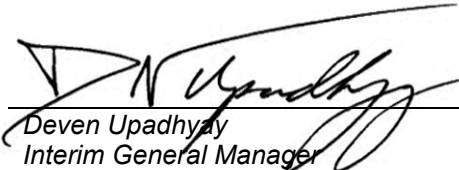
This action authorizes ~~\$5.756~~ million for the co-managed support services for the operation and maintenance of the Metropolitan Cybersecurity Operations Center. The total project budget includes funds for awarding a new contract with CAI for ~~\$5.756~~ million for professional and technical services.

Project Milestone(s)

March 2025:	Onboard of co-managed service vendor and transition to co-managed services and 24x7x365 monitoring coverage
June 2025:	Co-managed services vendor fully integrated with Metropolitan CSOC and conducting cybersecurity operational support services.



Charles Eckstrom
Group Manager, Information Technology
2/4/2025
Date



Deven Upadhyay
Interim General Manager
2/4/2025
Date