THE METROPOLITAN WATER DISTRICT OF SOUTHERN CALIFORNIA

BOARD ACTION

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

8/15/2023 Board Meeting

8-2

Subject

Authorize an agreement with Computer Aid Incorporated in an amount not to exceed $1,750,000 to provide staff augmentation support services for the operation and maintenance of the Metropolitan Cybersecurity Operations Center for a period of up to one year; the General Manager has determined that the proposed action is exempt or otherwise not subject to CEQA **[Consultation with Metropolitan Director of Info Tech Services, Information Technology, Jacob Margolis, or designated agents on threats to public services or facilities; may be heard in closed session pursuant to Gov. Code Section 54957(a)]**

Executive Summary

This action awards an agreement for operation and maintenance of Metropolitan's enterprise-wide Cybersecurity Operations Center (CSOC) for up to a one-year period. The purpose of this contract is to provide basic cybersecurity threat monitoring capability while Metropolitan republishes an RFP for a long-term cybersecurity operations center managed services contract. 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 will function 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.

Timing and Urgency

This action will authorize the General Manager to proceed with an agreement with Computer Aid Incorporated (CAI) to provide minimal staffing to achieve basic continuous monitoring for cyber threats while the RFP process for a more comprehensive service can be released and awarded to a vendor for a long-term managed services contract.

Details

Background

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 will be required to conduct the continuous operation.

The CSOC will centrally monitor, detect, analyze, mitigate, and respond to cyber threats on the Metropolitan Enterprise Information Technology and Supervisory Control and Data Acquisition (SCADA) systems. Currently, multiple groups at Metropolitan and external parties independently gather and analyze information from data centers, the disaster recovery facility, workstation networks, physical security, supervisory control, and data acquisition (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 (CERTs) and Information

Sharing and Analysis Centers (ISACs). Correlating this data to find suspicious activity can be extremely challenging and often only occurs long after a cyber event or incident happens.

To meet this requirement, 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 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 for fiscal biennial 2022-2024.

Objective

CAI would be required 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 shall provide 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 shall be established in accordance with the guiding principles of security established by the National Institute of Standards and Technology (NIST), 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 (WAN), local area networks (LAN), 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.

Professional Services Required

Metropolitan used RFQ 1303 for Information Technology On-Call services. CAI was one of the vendors selected under the cybersecurity category under RFQ 1303.

CAI shall assist Metropolitan in staffing and monitoring its CSOC by supporting operations 24 hours per day, seven days per week, 365 days per year, with provision for on-call support during holiday periods. CAI staff will work under the direction of a CAI Service Delivery Manager, who will be providing services at the direction of the Metropolitan CSOC Team Manager and Office of Enterprise Cybersecurity.

Work shall be performed at the primary Metropolitan CSOC facility. CAI personnel shall operate from the Metropolitan CSOC facilities. Metropolitan will coordinate clearance for and grant physical access by qualified and cleared personnel into the CSOC premises and facilities and into other Metropolitan sites.

This action authorizes $1,750,000 for CAI to provide staff augmentation services for the operation and maintenance of the CSOC. The total project budget includes funds for awarding a new contract with CAI for a nine-month period for $1,312,500 with an option to extend month to month at $145,833.33 per month up to a total one-year period. See **Attachment 1** for the Financial Statement.

Project Milestones

September 1, 2023 – Onboarding

October 1, 2023 – Conducting CSOC Monitoring

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

By Minute Item 52778, dated April 12, 2022, the Board appropriated a total of $600 million for projects identified in the Capital Investment Plan for Fiscal Years 2022/23 and 2023/24.

California Environmental Quality Act (CEQA)

CEQA determination for Option #1:

The proposed action is not defined as a project under CEQA (Public Resources Code Section 21065, State CEQA Guidelines Section 15378) because it involves continuing administrative activities, such as general policy and procedure making, which will not cause either a direct physical change in the environment or a reasonably foreseeable indirect physical change in the environment (Section 15378(b)(2) of the State CEQA Guidelines).

CEQA determination for Option #2:

None required

Board Options

Option #1

Authorize an agreement with Computer Aid Incorporated in an amount not to exceed $1,750,000 to provide staff augmentation support services for the operation and maintenance of the Metropolitan Cybersecurity Operations Center for a period of up to one year.

Fiscal Impact: Expenditure of $1,750,000 in O&M funds
Business Analysis: This option will initiate implementation of security recommendations made by internal staff and DHS and will provide minimal ability to monitor for cyber threats affecting business computer systems and SCADA systems. This approach will comprehensively strengthen Metropolitan's cybersecurity to a minimal staffing level while the RFP process is reinitiated for a permanent CSOC co-managed service.

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.

Staff Recommendation

Option #1

7/25/2023

Charlie Eckstrom *Date*
Group Manager, Information Technology

7/30/2023

Adel Hagekhalil *Date*
General Manager

Attachment 1 – Financial Statement

Ref#it12686126

Allocated Funds for Cybersecurity Operations Center

	Current Board Action (Aug. 2023)
Labor	
Studies & Investigations	$ -
Final Design	-
Owner Costs (Program mgmt.)	-
Submittals Review & Record Drwgs	-
Construction Inspection & Support	-
Metropolitan Force Construction	-
Materials & Supplies	-
Incidental Expenses	-
Professional/Technical Services	1,750,000
Equipment Use	-
Contracts	-
Remaining Budget	-
Total	**$ 1,750,000**