THE METROPOLITAN WATER DISTRICT
OF SOUTHERN CALIFORNIA

Board Report

Office of the General Auditor

- **General Auditor's Report for September 2025**

Summary

This report highlights significant activities of the Office of the General Auditor for the month ended September 30, 2025.

Purpose

Informational

Attachments

One report was issued during this period:

1. Cybersecurity Audit: Inventory & Control of IT Software Assets

Detailed Report

Audit & Advisory Projects

Twenty-five projects are in progress:

- Seven audit projects are in the report preparation phase.
    - One collaboration draft report was issued: Cybersecurity Audit: Inventory & Control of SCADA Network Assets
- Eighteen projects are in the execution phase, including eight audits and ten advisories.

No management responses are outstanding.

Follow-Up Reviews

Twelve projects are in the follow-up phase:

- Seven follow-up reviews are in progress.
- Five follow-up reviews have not been started.

No follow-up review forms are overdue.

Report Details

1. **Cybersecurity Audit: Inventory & Control of IT Software Assets** issued September 30, 2025
    - Audit scope included software managed by the Information Technology Group and installed on Metropolitan's business network as of March 31, 2025.
    - Three (3) recommendations with the following rating: three Priority 2.

Date of Report: October 14, 2025

Other General Auditor Activities

1. **Internal Quality Assessment**
   Preparation for the annual internal quality assessment, as required by professional internal auditing standards, is in progress. Surveys were distributed to the Board, management, and department staff.

2. **External Resources RFQ**
   Evaluation of submittals received for the specialty internal audit services RFQ is in process.

3. **External Auditor Support**
   Assistance to external auditor Macias Gini & O’Connell LLP continues in accordance with their work plan.

4. **Global Internal Audit Standards**
   Evaluation and adoption of the updated standards issued by the Institute of Internal Auditors, effective January 9, 2025, is in progress. Board roles and responsibilities, per the Standards, were presented as an information item at the September meeting of the Audit Committee.

5. **Training**
   Staff attended Beyond Compliance: Driving Impactful Change as Public Sector Internal Auditors training.

6. **Joint Classification Study Session**
   Participated in a focus group session as part of the 2025 Joint Classification and Compensation Study, a collaborative effort between the District and AFSCME, for the Deputy Auditor series.

Office of the General Auditor

Cybersecurity Audit: Inventory & Control of IT Software Assets

Project Number: 23-35
September 30, 2025

THE METROPOLITAN WATER DISTRICT OF SOUTHERN CALIFORNIA

PUBLIC INFORMATION

TABLE OF CONTENTS

Executive Summary

BACKGROUND

The Center for Internet Security (CIS) is a community-driven nonprofit that has developed the CIS Controls and CIS Benchmarks, which are globally recognized best practices for securing IT systems and data. Its mission is “to make the connected world a safer place by developing, validating, and promoting timely best practice solutions that help people, businesses, and governments protect themselves against pervasive cyber threats.” Organizations can implement the CIS Critical Security Controls (CIS Controls), a set of 18 controls with detailed safeguards, to improve their cybersecurity posture.

One of these controls is the Inventory and Control of Software Assets, which requires organizations to actively inventory, track, and manage all software installed across their networks. This control ensures that only authorized software can execute, while unauthorized or unmanaged software is detected and prevented from installation or use.

WHAT WE DID

Our audit scope included software installed on Metropolitan’s business network and managed by the Information Technology Group as of March 31, 2025.

Our audit objective was to determine whether all software on the network is actively managed (i.e., inventoried, tracked, and corrected) to reduce the risk of attack.

WHAT WE CONCLUDED

[REDACTED]

WHAT WE RECOMMEND

[REDACTED]

Management agreed with our observations and recommendations.

Information has been removed from this Executive Summary as it contains an assessment of Metropolitan’s vulnerability to terrorist attack or other criminal acts intended to disrupt Metropolitan’s operation and is for distribution or consideration in a closed session and not subject to the California Public Record Act pursuant to Government Code Section 7929.200.

NUMBER OF RECOMMENDATIONS

0	PRIORITY 1	Response time: Immediate
3	PRIORITY 2	Response time: Within 90 days
0	PRIORITY 3	Response time: Within 180 days

THE METROPOLITAN WATER DISTRICT
OF SOUTHERN CALIFORNIA

Date: September 30, 2025

To: Audit Committee

From: Scott Suzuki, CPA, CIA, CISA, CFE, General Auditor

Subject: Cybersecurity Audit: Inventory & Control of IT Software Assets
(Project Number 23-35)

We have completed a cybersecurity audit of inventory and control of IT software assets for the Information Technology Group.

Due to the sensitive nature of the critical infrastructure information, details of our observations and recommendations were shared with select members of the Board and management in a separate confidential report not subject to public release.

Supplemental information, including our scope and objectives, is included in Appendix A. Appendix B includes a description of our new recommendation priority rating system.

We appreciate the courtesies and cooperation provided by the Information Technology Group.

The results in this report will be summarized for inclusion in a status report to the Board. If you have any questions regarding our audit, please do not hesitate to contact me directly at 213.217.6528 or Assistant General Auditor Kathryn Andrus at 213.217.7213.

Attachments

cc: Board of Directors
General Manager
General Counsel
Ethics Officer
Office of the General Manager Distribution
Assistant General Managers
External Affairs Distribution
Information Technology Group Distribution
External Auditor

RESULTS

The Recognition, Results Overview, and Observations & Recommendations sections have been removed from this report as they contain an assessment of Metropolitan's vulnerability to terrorist attack or other criminal acts intended to disrupt Metropolitan's operation and are for distribution or consideration in a closed session and not subject to the California Public Records Act pursuant to Government Code Section 7929.200.

EVALUATION OF MANAGEMENT'S RESPONSE

Internal Audit considers management's response appropriate to the recommendations.

AUDIT TEAM

Sherman Hung, CISA, Principal Auditor

APPENDIX A: SUPPLEMENTAL INFORMATION

SCOPE & OBJECTIVES

Our audit scope included software managed by the Information Technology Group and installed on Metropolitan's business network as of March 31, 2025.

Our audit objective was to determine whether all software on the network is actively managed (i.e., inventoried, tracked, and corrected) to reduce the risk of attack.

EXCLUSIONS

Our audit scope did not include the software/application systems that are on SCADA networks or are under development.

PRIOR AUDIT COVERAGE

We have not completed any audits with a similar scope within the last five years.

AUTHORITY

We performed this audit in accordance with the General Auditor's Internal Audit Plan for FY 2024/25 approved by the Board.

PROFESSIONAL INTERNAL AUDIT STANDARDS

Our audit was conducted in conformance with the International Standards for the Professional Practice of Internal Auditing issued by the International Internal Audit Standards Board.

FOLLOW-UP REVIEWS

The Office of the General Auditor has implemented a new follow-up process to ensure management has effectively implemented corrective action related to our recommendations. Management is required to report recommendation implementation status to our office within six months following the issuance of this report, and a first follow-up review will occur shortly thereafter. All audit recommendations are expected to be implemented within a year of this report, and if necessary, a second follow-up review will occur approximately six months after issuance of the first follow-up review report. Any audit recommendations not implemented after the second follow-up review will be shared with the Board/Audit Committee at its next scheduled meeting.

INTERNAL CONTROL SYSTEM

An internal control system is a continuously operating and integrated component of Metropolitan's operations. Internal controls are implemented by the Metropolitan management and seek to provide reasonable (not absolute) assurance that Metropolitan's business objectives will be achieved. However, limitations are inherent in any internal control system, no matter how well designed, implemented, or operated. Because of these limitations, errors or irregularities may occur and may not be detected.

Specific examples of limitations include, but are not limited to, poor judgment, carelessness, management override, or collusion. Accordingly, our audit would not necessarily identify all internal control weaknesses or resultant conditions affecting operations, reporting, or compliance. Additionally, our audit covers a point in time and may not be representative of a future period due to changes within Metropolitan and/or external changes impacting Metropolitan.

METROPOLITAN'S RESPONSIBILITY FOR INTERNAL CONTROL

It is important to note that Metropolitan management is responsible for designing, implementing, and operating a system of internal control. The objectives of internal controls are to provide reasonable assurance as to the reliability and integrity of information; compliance with policies, plans, procedures, laws, and regulations; the safeguarding of assets; the economic and efficient use of resources; and the accomplishment of established goals and objectives. In fulfilling this responsibility, management judgment is required to assess the expected benefits and related costs of internal control policy and procedures and to assess whether those policies and procedures can be expected to achieve Metropolitan's operational, reporting, and compliance objectives.

APPENDIX B: PRIORITY RATING DEFINITIONS

The Office of the General Auditor utilizes a priority rating system to provide management a measure of urgency in addressing the identified conditions and associated risks. We assess the significance of each observation identified during the audit using professional judgment and assign priority ratings to each recommendation using the criteria listed below. Factors taken into consideration in assessing the priority include the likelihood of a negative impact if not addressed, the significance of the potential impact, and how quickly a negative impact could occur.

	PRIORITY		
Definition	Observation is *serious* enough to warrant *immediate* corrective action. The condition may represent a serious financial, operational, or compliance risk. A priority 1 recommendation may result from a key control(s) being absent, not adequately designed, or not operating effectively.	Observation is of a *significant* nature and warrants *prompt* corrective action. It may represent a moderate financial, operational, or compliance risk. A priority 2 recommendation may result from a process or less critical control(s) not being adequate in design and/or not operating effectively on a consistent basis.	Observation involves an internal control issue or compliance lapse that can be corrected in the *timely* course of normal business. A priority 3 recommendation may result from a process or control that requires enhancement to better support Metropolitan's objectives and manage risk.
Response Time	Immediate	Within 90 Days of report issuance	Within 180 Days of report issuance

APPENDIX C: MANAGEMENT'S RESPONSE

The Management Response has been removed from this report as it contains an assessment of Metropolitan's vulnerability to terrorist attack or other criminal acts intended to disrupt Metropolitan's operation and is for distribution or consideration in a closed session and not subject to the California Public Records Act pursuant to Government Code Section 7929.200.