Los Angeles County
Metropolitan Transportation
Authority
One Gateway Plaza
3rd Floor Board Room
Los Angeles, CA

Metro

# Board Report

**File #:** 2024-0245, **File Type:** Program **Agenda Number:** 25.

**FINANCE, BUDGET, AND AUDIT COMMITTEE**
**JULY18, 2024**

**SUBJECT: CYBERSECURITY LIABILITY INSURANCE PROGRAM**

**ACTION: APPROVE RECOMMENDATION**

## RECOMMENDATION

AUTHORIZE the Chief Executive Officer to negotiate and purchase a cybersecurity liability insurance policy with up to $50 million in limits at a cost not to exceed $3.850 million for the 12-month period effective September 1, 2024, to September 1, 2025.

## ISSUE

Metro's cybersecurity liability insurance policy expires on September 1, 2024. Insurance underwriters will not commit to final pricing until three weeks before the current program expires. Consequently, staff requests a not-to-exceed amount for this renewal pending final pricing. Metro purchases an insurance policy to cover cybersecurity liability exposures. Cybersecurity is the practice of being protected against criminal or unauthorized use of systems and electronic data. These exposures include but are not limited to:

- Unavailability of IT systems and networks
- Physical asset damage and associated loss of use
- Loss or deletion of data
- Data corruption or loss of data integrity
- Data breach leading to compromise of third-party confidential/personal data
- Cyber espionage resulting in the release of confidential/sensitive information
- Extortion demands to cease a cyber-attack
- Direct financial loss due to theft
- Damage to reputation
- Bodily injury/property damage to third parties

Without this insurance, Metro is subject to unlimited liability for claims resulting from a cyber-attack or data breach event.

## BACKGROUND

FY23 was the first year Metro purchased cybersecurity liability coverage. For this current renewal,

USI Insurance Services ("USI"), the insurance broker for Metro, was requested to market Metro's cybersecurity liability insurance program to qualified insurance carriers. Through its partnership with Howden, a London broker, USI has received quotes from the incumbent carrier, which has A.M. Best ratings indicative of acceptable financial soundness and ability to pay claims. The premium indications below are based on current market expectations. The quotes expire on September 1, 2024.

USI provides a not-to-exceed number that serves three functions. First, the number provides an amount to cover the recommended premium and contingency that Risk Management can bring to the CEO and Board to obtain approval for the binding of the program. Second, the number allows Metro's broker ample time to continue negotiating with underwriters to ensure that Metro obtains the most competitive pricing available. Third, the not-to-exceed amount allows Metro to secure the quoted premium during the board cycle process before quote expiration.

## DISCUSSION

Public entities continue to be a target for cyber-attacks. According to Verizon's Data Breach Investigation Report: 20% of all incidents reported in 2023 were related to the Public Entity Sector, which was more than any other sector. A robust cybersecurity program could help reduce the number of successful cyber-attacks and financial risks associated with doing business online by 1) promoting the adoption of preventative measures in return for more coverage and 2) encouraging the implementation of best practices by basing premiums on an insured's level of self-protection.

The cyber insurance market has matured somewhat with increased discipline in underwriting and reduced deployment of capacity where controls and security protocols are perceived to be ineffective at adapting to security threats. Those who have implemented stronger cybersecurity measures will see a more mature market with softer price hikes for those clients who can demonstrate strong protocols throughout their systems.

There have been changes in the regulatory environment around cybersecurity, specifically for public transit organizations. In February of 2023, the Federal Transit Administration (FTA) published a cybersecurity assessment tool for transit agencies to help guide them in identifying and mitigating risk. FTA continues to guide cybersecurity activities and supports the U.S. Department of Homeland Security (DHS) in promoting enhanced security for transit agencies. Additionally, as a condition under 49 U.S.C. 5323(v), rail transit operators must certify that they have a process to develop, maintain, and execute a plan for identifying and reducing cybersecurity risks. The general guidance is built around the National Institute of Standards and Technology (NIST) Cyber Security Framework. With Metro's vast network of third-party service providers, this is a major exposure area that needs to be continually monitored on an ongoing basis.

Multiple questionnaires and interviews are required by Metro's information security and Supervisory Control and Data Acquisition (SCADA) team's experts on the systems and network controls. A proposal of coverage for cybersecurity liability insurance based on the findings and the insurance carrier's knowledge of Metro's internal controls is provided. The proposed program, from carrier BRIT Re, a Lloyds of London consortium, provides up to $50 million in excess coverage on a claims-made basis with a $10 million self-insured retention (SIR). Attachment A summarizes the premium options,

and Attachment B summarizes the coverages. The proposal was reviewed by Risk Management and Information Technology Services (ITS) team members, who agree the proposed coverage will help mitigate Metro's financial and reputational risk should the agency experience a cyber-attack event.

## DETERMINATION OF SAFETY IMPACT

Approval of this recommendation to purchase a cybersecurity liability insurance policy will not directly impact the safety of Metro's patrons or employees. The policy will limit Metro's liability for claims resulting from a cyber-attack or data breach event. Additionally, the policy will aid in Metro's recovery and moderate financial losses as well as harm to Metro's reputation resulting from cyber events and incidents.

## FINANCIAL IMPACT

Funding for ten months, or $3,208,333, for this action is included in the FY25 Budget in cost center 0531, Risk Management -- Non-Departmental Costs, under projects 100001 - General Overhead, 300022 - Rail Operations - Blue Line, 300033 - Rail Operations - Green Line, 300044 - Rail Operations - Red Line, 300066 - Rail Operations - Expo Line, 300077 - Crenshaw Line, 301012 - Metro Orange Line, 306001 - Operations Transportation, 306002 - Operations Maintenance, 320011 - Union Station and 610061 - Owned Property in account 50699 (Ins Prem For Other Ins). Additional funding to cover premium costs beyond FY25 budgeted amounts will be addressed by fund reallocations during the year.

The remaining two months of premium will be requested during the FY26 Budget development cycle.

Impact to Budget

The source of funding for this action will come from federal, state, and local funding sources that are eligible for bus and rail operations.

## EQUITY PLATFORM

The proposed action supports Metro's ability to safely serve the communities and customers who rely on Metro's transportation services and assets by providing insurance coverage that will allow Metro to more quickly resume operations in the event of a cybersecurity breach.

## IMPLEMENTATION OF STRATEGIC PLAN GOALS

The recommendation supports strategic plan goal # 5, "Provide responsive, accountable, and trustworthy governance within the LA Metro organization." The responsible administration of Metro's risk management programs includes the use of insurance to mitigate large financial risks resulting from cybersecurity events.

## ALTERNATIVES CONSIDERED

As outlined in Attachment A, various coverage limits were considered for the cybersecurity liability

insurance program. All options include a SIR of $10 million for the same program. Option A, Metro's current limit, provides $50 million in coverage, Option B provides $75 million, and Option C provides $100 million in coverage.

Option A is recommended as the best value option while retaining a reasonable amount of risk over the coverage limit.

## NEXT STEPS

Upon Board approval of this action, staff will advise USI to proceed with the placement of the cybersecurity liability insurance program outlined herein, effective September 1, 2024.

## ATTACHMENTS

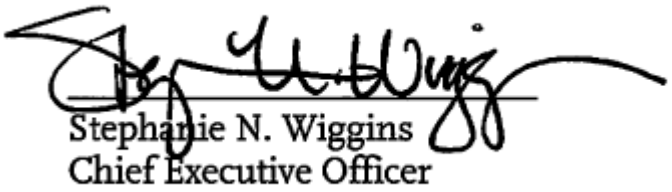
Attachment A - Coverage Options and Premiums

Attachment B - Coverage Description

Prepared by: William Douglas, Senior Manager Risk Financing, (213) 922-2105

Bryan Sastokas, Deputy Chief Information Technology Officer, (213) 922-5510

Reviewed by: Kenneth Hernandez, Interim Chief Safety Officer, (213) 922-2990



Stephanie N. Wiggins
Chief Executive Officer