



## Board Report

File #: 2025-0345, File Type: Program

Agenda Number: 21.

### FINANCE, BUDGET, AND AUDIT COMMITTEE JULY 17, 2025

**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 not-to-exceed premium of \$3.104 million for the 12-month period effective September 1, 2025, to September 1, 2026.

#### **ISSUE**

Metro's cybersecurity liability insurance policy will expire on September 1, 2025. Insurance underwriters will not commit to final pricing until three weeks before the current program expires. Consequently, we are requesting 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**

For this current renewal, Marsh USA, LLC (Marsh), the insurance broker for Metro, was requested to

---

market Metro's cybersecurity liability insurance program to qualified insurance carriers. Marsh, through its partnership with Howden, a London broker, 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 provided are based on current market expectations and expire on September 1, 2025.

Marsh's not-to-exceed premium serves three functions. First, it 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 our broker ample time to continue negotiating with underwriters to ensure Metro obtains the most competitive pricing. And third, the not-to-exceed amount allows Metro to secure the quoted premium during the board cycle process prior to quote expiration.

## **DISCUSSION**

Public entities continue to be targeted for cyber-attacks as the cyber risk environment evolves. According to *The State of Ransomware in the U.S.*, at least 50 local governments in the U.S. experienced ransomware attacks in the first half of 2024. Marsh observed a 16% increase in the number of cyber notifications from 2023 to 2024, underscoring the growing complexity of cyber risks. The frequency of cyber events and claim notifications in 2024 is primarily driven by third-party events, such as the CrowdStrike outage (July, 2024).

A new concern is the use of Generative AI and its ability to amplify existing cyber risks, leading to potential consequences, including business interruptions from AI system failures and inadvertent copyright infringements. The unpredictability of third-party events and the evolving cyber risk environment highlights the need for strong cybersecurity controls and effective insurance.

In Q1 of 2025, cyber insurance clients' rates decreased by 4% on average, marking the eighth consecutive quarter of reductions. This favorable environment has led clients to utilize premium savings to purchase higher limits, reduce retentions, shorten waiting periods, and broaden coverage.

Public entities with strong cyber risk controls have the greatest advantage in the current marketplace. Adhering to guidelines set forth by agencies such as the Federal Transit Administration (FTA) and the Cybersecurity and Infrastructure Security Agency (CISA) is critical for public entities like Metro. These organizations provide cybersecurity frameworks, risk assessments, and audits for public entities to comply with.

Metro has completed the Marsh Cyber Self-Assessment, which provides a review of cybersecurity controls. Marsh's analytics suggest purchasing between \$40 million and \$85 million. The proposed program, from carrier BRIT Re, a Lloyd's 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 that 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 action positively impacts the safety of Metro's patrons and employees. Cyber Liability insurance carriers will review cybersecurity procedures to mitigate potential risks or hazards and provide an overall risk assessment of Metro's practices and assets as they underwrite the program. Carriers may provide best-practice guidance to enhance Metro's risk profile, and the policy will limit Metro's liability for claims resulting from a cyber-attack or data breach event. Additionally, the policy will aid Metro's recovery and moderate financial losses, as well as harm to Metro's reputation resulting from cyber events and incidents.

## **FINANCIAL IMPACT**

The FY26 Budget includes \$3.01 million for this action in cost center 0531, Non-Departmental - Ops Risk Management, under projects 100001 - General Overhead, 300022 - Rail Operations - A Line, 300033 - Rail Operations - C Line, 300044 - Rail Operations - B Line, 300066 - Rail Operations - E Line, 300077 - K Line, 301012 - G Line, 306001 - Operations Transportation, 306002 - Operations Maintenance, 320011 - Union Station and 610061 - Owned Property.

Metro's insurance premiums are amortized and span two fiscal years. The cost center manager and the Interim Chief Transit Safety Officer will be accountable for budgeting in FY27 costs not included in the FY26 budget.

### **Impact to Budget**

The sources of funding for this action will come from federal, state, and local resources 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.

## **VEHICLE MILES TRAVELED OUTCOME**

VMT and VMT per capita in Los Angeles County are lower than national averages, the lowest in the SCAG region, and on the lower end of VMT per capita statewide, with these declining VMT trends due in part to Metro's significant investment in rail and bus transit.\* Metro's Board-adopted VMT reduction targets align with California's statewide climate goals, including achieving carbon neutrality by 2045. To ensure continued progress, all Board items are assessed for their potential impact on VMT.

While this item does not directly encourage taking transit, sharing a ride, or using active transportation, it is a vital part of Metro operations, as it provides cybersecurity liability coverage for Metro's assets. Because the Metro Board has adopted an agency-wide VMT Reduction Target, and this item supports the agency's overall function, it is consistent with the goals of reducing VMT.

\*Based on population estimates from the United States Census and VMT estimates from Caltrans' Highway Performance Monitoring System (HPMS) data between 2001-2019.

## **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**

Various limits of coverage were considered, as outlined in Attachment A, for the cybersecurity liability program. All options include an SIR of \$10 million for the same program. Option A, Metro's current limit, provides \$50 million in coverage, Option B provides \$75 million in coverage, and Option C provides \$100 million in coverage.

Option A, which is within Marsh's analytics limits range, is recommended as the best value option while retaining a reasonable amount of risk over the coverage limit.

## **NEXT STEPS**

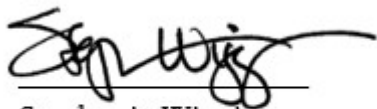
Upon Board approval of this action, staff will advise Marsh to proceed with the placement of the cybersecurity liability insurance program outlined herein, effective September 1, 2025.

## **ATTACHMENTS**

Attachment A - Coverage Options and Premiums  
Attachment B - Coverage Description

Prepared by: William Douglas, Senior Manager, Risk Financing, (213) 922-2105  
Claudia Castillo del Muro, Executive Officer, Risk Management, (213) 922-4518  
Bryan Sastokas, Deputy Chief Information Technology Officer, (213) 922-5510

Reviewed by: Kenneth Hernandez, Interim Chief Risk, Corporate Safety, and Asset Management Officer, (213) 922-2990

A handwritten signature in black ink, appearing to read 'Step Wiggins', written over a horizontal line.

Stephanie Wiggins  
Chief Executive Officer

ATTACHMENT A

Coverage Options and Premiums

Carrier: BRIT Re

Cyber Security Insurance Program Premium and Proposed Options

|                                 | CURRENT<br>PROGRAM | OPTIONS     |             |             |
|---------------------------------|--------------------|-------------|-------------|-------------|
|                                 |                    | A           | B           | C           |
| Self-Insured<br>Retention (SIR) | \$10 mil           | \$10 mil    | \$10 mil    | \$10 mil    |
| Limit of Coverage               | \$50 mil           | \$50 mil    | \$75 mil    | \$100 mil   |
| Premium *                       | \$2,735,229        | \$3,104,430 | \$4,024,020 | \$4,643,100 |

|                                   |             |             |             |
|-----------------------------------|-------------|-------------|-------------|
| Not to Exceed                     | \$3,104,430 | \$4,024,020 | \$4,643,100 |
| Premium per mil coverage \$54,705 | \$62,089    | \$53,634    | \$46,431    |

\* Includes commissions, taxes and fees.

**Coverage Description**

Marsh USA, LLC (Marsh) provided a proposal of coverage for cyber liability insurance. The following summarizes the coverages and exclusions:

**Included Coverage**

| <b>Exposure</b>                                             | <b>Brief Description</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SECURITY AND PRIVACY LIABILITY (INCLUDING EMPLOYEE PRIVACY) | Covers the insured's liability for damages resulting from a data breach. Such liability most often results from (1) loss, theft, or unauthorized disclosure of personally identifiable information (PII) in the insured's care, custody, and control; (2) damage to data stored in the insured's computer systems belonging to a third party; (3) transmission of malicious code or denial of service to a third party's computer system; (4) failure to timely disclose a data breach; (5) failure of the insured to comply with its own privacy policy prohibiting disclosure or sharing of PII; and (6) failure to administer an identity theft program required by governmental regulation or to take necessary actions to prevent identity theft. In addition, this insuring agreement covers the cost of defending claims associated with each of these circumstances |
| SECURITY BREACH RESPONSE COVERAGE                           | Coverage for the expenses involved in responding to a data breach. These include legal expenses, forensic experts, costs to notify affected parties and provide credit monitoring, and public relations expenses to mitigate reputational damage.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| PRIVACY REGULATORY CLAIMS COVERAGE                          | The insuring agreement covers the costs of dealing with state and federal regulatory agencies (which oversee data breach laws and regulations), including (1) the costs of hiring attorneys to consult with regulators during investigations and (2) the payment of regulatory fines and penalties that are levied against the insured (as a result of the breach).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| PCI-DSS ASSESSMENT COVERAGE                                 | Payment Card Industry Data Security Standard (PCI DSS) was formed around 2004 by the major credit card companies to establish guidelines in the handling and processing of transactions including personal information. The policy will provide coverage for assessments, fines or penalties imposed by banks or credit card companies due to non-compliance with the Payment Card Industry                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

|                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                          | Data Security Standard (PCI DSS) or payment card company rules.                                                                                                                                                                                                                                                                                                                                                                                                                          |
| CYBER EXTORTION COVERAGE                                 | Cyber extortion is an online crime in which hackers hold your data, website, computer systems, or other sensitive information hostage until you meet their demands for payment. The policy will cover the cost to investigate a ransomware attack and negotiate with the hackers.                                                                                                                                                                                                        |
| MULTIMEDIA LIABILITY                                     | Multimedia Liability provides coverage for third-party liability claims alleging damage resulting from dissemination of media material. This covers both electronic and non-electronic media material and may include claims of copyright or trademark infringement. libel.                                                                                                                                                                                                              |
| DIGITAL ASSET RESTORATION COSTS                          | Digital assets loss occurs when company data or software is corrupted or destroyed because of a network security failure. This type of loss can come because of an outside network breach or an inside job carried out by an employee. The policy covers the reasonable and necessary cost to replace, restore or re-collect digital property from written or electronic records. Additionally, investigation expenses such as disaster recovery and computer forensics is also covered. |
| BUSINESS INCOME LOSS RESULTING FROM A NETWORK DISRUPTION | Business Interruption covers business income loss and extra expenses incurred during a computer network outage. The coverage applies to outages of <i>internally managed IT</i> , such as employee                                                                                                                                                                                                                                                                                       |
|                                                          | devices or internal networks or databases -- not a cloud computing provider or other type of third-party IT vendor.                                                                                                                                                                                                                                                                                                                                                                      |
| Bodily Injury                                            | Injury to persons (including death)                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

### **Excluded Coverage**

The proposal of coverage also indicates various exclusions or exposures that will not be covered:

| <b>Exposure</b>                        | <b>Brief Description</b>                                                                                                                                                                                                                                                                                                                   |
|----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| BUSINESS INCOME LOSS (Physical Damage) | Some insurers have brought forward business interruption coverage as part of cyber insurance or as stand-alone business interruption insurance policies. There doesn't have to be a complete shutdown to trigger the coverage. Instead, a system slowdown due to network issues or malicious elements can also be classified as a trigger. |

|                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                   | However, the proposal indicates there will be no coverage for physical damage BI claims.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| ENSUING PROPERTY DAMAGE LOSS                      | Exception to an exclusion in a first-party property policy that applies in a special type of fact pattern where the damage caused by an excluded peril operates as a link in the "chain of events" that enables a covered peril to damage other property. (proximate cause) Symbolically, a classic ensuing loss fact pattern can be represented as follows: <i>excluded peril - excluded damage - covered peril - ensuing damage</i> . Note that there must be two kinds of damages—an initial loss and an ensuing loss. Most courts will not apply an ensuing loss provision if an excluded peril caused a covered peril that results in only one kind of damage. |
| Inspection and Loss Prevention/Mitigation Expense | Loss prevention aims to reduce the possibility of damage and lessen the severity if such a loss should occur.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Debris Removal                                    | Debris removal insurance is a section of a property insurance policy that provides reimbursement for clean-up costs associated with damage to property.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |



# Cybersecurity Liability Insurance Program

Finance, Budget, and Audit Committee

July 17, 2025

File #2025-0345



Metro

# Cybersecurity Liability Insurance Program

## 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 \$3.104 million for the 12-month period effective September 1, 2025, to September 1, 2026.

## 2025-2026 Renewal Program

Aggregate Limit of Liability: \$50M  
Brit UK (Lloyd's)  
Annual Premium (NTE): \$3.104M

\$10M/14 Days - Retention

# Cyber Coverage Features

## **First Party Events/Losses:**

- Breach Response
  - Forensic/Legal Costs
  - Crisis Management & Notification Costs
- Cyber Extortion/Ransomware
- Business Service & System Disruption Losses
- System & Service Failure Losses
- Data Recovery, Restoration, & Digital Restoration Expenses
- Cyber Crime Losses

## **Third Party & Regulatory Liability Claims:**

- Enterprise Security Event Liability
- Privacy Regulatory Liability
- Media Liability
- PCI Fines & Penalties

# Renewal Marketing and Coverage Options

## Coverage Options and Premiums

Carrier: BRIT Re

### Cyber Security Insurance Program Premium and Proposed Options

|                                 | CURRENT<br>PROGRAM | OPTIONS     |             |             |
|---------------------------------|--------------------|-------------|-------------|-------------|
|                                 |                    | A           | B           | C           |
| Self-Insured<br>Retention (SIR) | \$10 mil           | \$10 mil    | \$10 mil    | \$10 mil    |
| Limit of Coverage               | \$50 mil           | \$50 mil    | \$75 mil    | \$100 mil   |
| Premium *                       | \$2,735,229        | \$3,104,430 | \$4,024,020 | \$4,643,100 |

|                                   |             |             |             |
|-----------------------------------|-------------|-------------|-------------|
| Not to Exceed                     | \$3,104,430 | \$4,024,020 | \$4,643,100 |
| Premium per mil coverage \$54,705 | \$62,089    | \$53,634    | \$46,431    |

\* Includes commissions, taxes and fees.



**Metro**



Thank you



Metro