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

File #: 2026-0442, **File Type:** Program **Agenda Number:** 25.

FINANCE, BUDGET, AND AUDIT COMMITTEE
JULY 16, 2026

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 $2.7 million for the 12-month period effective September 1, 2026, to September 1, 2027.

ISSUE

Metro's cybersecurity liability insurance policy expires September 1, 2026. Insurance underwriters will not commit to final pricing until three weeks before the current program expires. Consequently, staff recommends 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.

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 below are based on current market expectations and expire on September 1, 2026.

Marsh provides a not-to-exceed number that serves three functions. First, the number provides an amount to cover the recommended premium and contingency that staff can present to the Board to obtain approval for the binding of the program. Second, the number allows the broker ample time to continue to negotiate with underwriters to ensure that Metro obtains the most competitive pricing available. 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 Marsh's Cyber Risk Intelligence Center, of the over 1,300 cyber claims they have seen in 2025, 13% of those claims are related to ransomware incidents. Privacy and regulatory claims frequency are on the rise in connection with broader privacy regulations.

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 in coverage. The proposed program, from carrier BRIT Re, a Lloyd's of London consortium, provides up to $50 million in coverage on a claims-made basis with a $5 million self-insured retention (SIR). Attachment A summarizes the premium options, and Attachment B summarizes the coverages. .

DETERMINATION OF SAFETY IMPACT

Approval of this recommendation positively impacts the safety of Metro's patrons and employees. Cyber Liability insurance carriers will review security procedures utilized in cyber programs 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.

FINANCIAL IMPACT

Funding of $2.9 million for this action is included in the FY27 Adopted Budget in cost center 0531, Risk Management - Non Departmental Costs, 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 - Bus Operations - G Line, 306001 - Operations Transportation, 306002 - Operations Maintenance, 320011 - Union Station and 610061 - Owned Property.

Since this is a multi-year contract, the cost center manager and the Chief Risk, Corporate Safety, and Asset Management Officer will be accountable for budgeting the cost in the future year.

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 secure the resources required to respond to a cyber incident and ensure the integrity of internal and external data resources.

VEHICLE MILES TRAVELED OUTCOME

Vehicle Miles Traveled (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 service disruptions and financial risks resulting from cybersecurity events.

ALTERNATIVES CONSIDERED

Various limits of coverage were considered, as outlined in Attachment A, for the cybersecurity liability insurance program. All options include an SIR of $5 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, 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, 2026.

ATTACHMENTS

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

Prepared by: William Douglas, Director, Risk Management, (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:
Arnold Hackett, Senior Advisor to the Chief Executive Officer, (213) 922-7403
Kenneth Hernandez, Chief Risk, Corporate Safety, and Asset Management Officer, (213) 922-2990

Stephanie Wiggins
Chief Executive Officer

ATTACHMENT A

Coverage Options and Premiums

Carrier: BRIT Re

Cybersecurity Insurance Program Premium and Proposed Options

	CURRENT PROGRAM	OPTIONS		
		A	B	C
Self-Insured Retention (SIR)	$5 mil	$5 mil	$5 mil	$5 mil
Limit of Coverage	$50 mil	$50 mil	$75 mil	$100 mil
Premium *	$2,650,929	$2,650,929	$4,175,212	$5,000,000
Not to Exceed		$2,700,000	$4,200,000	$5,000,000

*Includes commissions, taxes and fees.

ATTACHMENT B

Coverage Description

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

Included Coverage

Exposure	Brief Description
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, trademark infringement, or 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 occur 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 are 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 internally managed IT, 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:

Exposure	Brief Description
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 business interruption 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: *excluded peril - excluded damage - covered peril - ensuing damage.* 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 16, 2026

File #2026-0442

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 $2.7 million for the 12-month period effective September 1, 2026, to September 1, 2027.

2026-2027
Renewal Program

Aggregate Limit of Liability: $50M
Brit UK (Lloyd's)
Annual Premium (NTE): $2.7M

$5M/14 Days – Self-Insured Retention (SIR)

Metro

Cybersecurity 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

Metro

Renewal Marketing and Coverage Options

Coverage Options and Premiums

Carrier: BRIT Re

Cyber Security Insurance Program Premium and Proposed Options

	CURRENT PROGRAM	OPTIONS		
		A	B	C
Self-Insured Retention (SIR)	$5 mil	$5 mil	$5 mil	$5 mil
Limit of Coverage	$50 mil	$50 mil	$75 mil	$100 mil
Premium *	$2,650,929	$2,650,929	$4,175,212	$5,000,000
Not to Exceed		$2,700,000	$4,200,000	$5,000,000

*Includes commissions, taxes and fees.

Metro

Thank you.

Metro