MOTION

As the second largest city in the nation, the entertainment capital of the world, one of the most sought after tourist destinations, one of the world's largest economies and home to the 2026 World Cup and 2028 Olympics, Los Angeles is a prime target for cyber-attacks.

Council File 22-0779 instructed the City's Information Technology Agency to report to the Council on the current and future deployment of the use of AI as a part of the City's Cybersecurity program as well as recommendations to improve the City's IT asset management capabilities. As mentioned by ITA's Chief Information Security Officer during an Information Technology & General Services Committee meeting on December 1, 2022, the City of Los Angeles analyzes approximately one billion security records and two million network intrusions every day. We are fortunate to have created an integrated Security Operations Center (SOC) in 2015, as well as the L.A. County Cyber Lab, and it is critical the City continues to be forward thinking and aware of new technologies introduced to better assist SOCs in their mission to efficiently detect, in real time, anomalistic behavior, which can be indicative of novel, never-before-seen, zero day attacks.

The general use of Artificial Intelligence (AI) by the City is not in question as ITA currently leverages various forms of Machine Learning and AI, aligning with the National Institute of Standards and Technology (NIST) cybersecurity framework. It was also recently made clear that AI is currently leveraged in the intrusion prevention and intrusion detection software in place today and has been effective at recognizing both known and unknown attacks. The mean time to detection and mean time to remediate these historical attacks is unclear.

What is also unclear is whether the City's detection capabilities are overly dependent on historical data, rules and threshold based detection, or human operators to ensure the tuning, care and feeding traditionally required to maintain a current and up-to-date security posture. Are we doing enough to protect ourselves from highly organized and well-funded organizations skilled at circumventing, with intent, rules and threshold based detection platforms? Are current detection systems predictive or reactive? Are we applying intelligence at the moment of observation or are we dependent on queries and investigation at some point after information has been collected, parsed, and stored and if so, how lengthy or costly is this investigation? Are we comparing ourselves to a historical baseline or looking ahead, recognizing anomalistic behavior in real time, and thus minimizing our mean time to detection and thus the immediacy of our response and are we deploying an effective asset management system capable of identifying vulnerabilities and take the appropriate action to close security gaps?

In an effort to ensure the City is doing all it can to protect its residents, employees, visitors, tourists and infrastructure, the City deserves the most current technology to predict and detect never-before-seen cyber-attacks, like zero-days, in real time using 3rd Wave AI and a comprehensive IT Asset Management System that helps ensure the City's assets are secure and protected from these threats.

I THEREFORE MOVE that the City Council direct ITA to identify at least one cybersecurity vendor using "third-wave artificial intelligence," as defined by the Defense Advanced Research Projects Agency (DARPA), and conduct a trial of this technology within the City's on-premise or cloud environment at no

19

cost to the City, reporting back to ITGS within 180 days with the results, such as the vendor's ability to detect and elevate true-positive threats and anomalies *without* relying on any rules, thresholds, historical training data or tuning to accomplish this, as well as the percentage of false-positive alerts their technology suppressed, and the amount of time and effort required to deploy, configure and maintain the system, both initially and ongoing.

I FURTHER MOVE that the City Council direct ITA to identify at least one cybersecurity vendor that can provide an IT Asset Management solution that could assist the City in easily and accurately discovering all of its IT assets across all environments as well as discovering security coverage gaps.

PRESENTED BY _____
JOHN S. LEE
Councilmember, 12th District

SECONDED BY _____

ORIGINAL