TED M. ROSS
GENERAL MANAGER
CHIEF INFORMATION OFFICER

MARYAM ABBASSI
ASSISTANT GENERAL MANAGER

BHAVIN PATEL
ASSISTANT GENERAL MANAGER

EDUARDO MAGOS
ASSISTANT GENERAL MANAGER

MARIA RAMOS
ACTING ASSISTANT GENERAL MANAGER

CITY OF LOS ANGELES

CALIFORNIA

KAREN BASS
MAYOR

INFORMATION TECHNOLOGY AGENCY

CITY HALL EAST
200 N. MAIN ST, ROOM 1400
LOS ANGELES, CA 90012
213.978.3311

ita.lacity.gov

July 27, 2026

REF: EXE-105-26

Honorable Members of the City Council
City of Los Angeles
Room 395, City Hall
Los Angeles, CA 90012

Attn: Government Operations Committee

SUBJECT: **RESPONSE TO BUDGET AND FINANCE COMMITTEE QUESTION 494 – 2026-27 PROPOSED BUDGET – CF 26-0600-S76**

CITYWIDE CYBERSECURITY GOVERNANCE: ROLES AND RESPONSIBILITIES

The City of Los Angeles utilizes a structured, multi-layered approach to cybersecurity governance to protect the digital assets entrusted to the City by its citizens, businesses, and visitors.

- **Executive Leadership (The Mayor's Office):** The City operates securely under the foundational mandates of Executive Directive No. 2. This directive established the overarching framework for protecting digital assets, securing network infrastructure, and mandating cybersecurity collaboration across the City.
- **Cyber Intrusion Command Center (CICC):** Established by Executive Directive No. 2, the CICC requires participation from all City departments. It serves as the central coordinating body designed to facilitate the sharing of risk management knowledge and best practices across multiple disciplines. The CICC Incident Response (IR) Team oversees citywide incident response planning and training.
- **Information Technology Agency (ITA):** As the central unifying technology department, ITA is key to the City's technology security strategy. The ITA manages the series of centralized cybersecurity defenses for Council-controlled departments (e.g. firewall, SIEM, vulnerability scans, Intrusion Prevention System, Intrusion Detection System, Endpoint Detection & Response, annual cybersecurity training, DHS Risk & Vulnerability assessments, etc) and citywide cybersecurity professionals (the Integrated Security Operations Center, ITA Security Office, etc). For departments that have been granted their own IT staffing and budget by City Council, the ITA requires those departments to comply with the citywide Information Security Policy and other CICC approved policies for any websites, applications, servers, or other digital assets deployed and maintained by that department.

- **Chief Information Security Officer (CISO):** The CISO serves as the Head of the ITA Information Security Office and chairs the activities of the CICC. Under normal daily operations, the CISO serves in a primarily oversight and governance capacity, providing strategic guidance, risk assessments, and policy direction to departments. However, in the event of an active cyber incident or attack, the CISO assumes a direct, authoritative role to coordinate the response, contain the threat, and manage the incident.
- **City Departments & Critical Asset Notification:** Every department plays a unique role in securing its own information and is responsible for the network usage of its employees. Crucially, departments must identify and document their mission-critical assets annually for the Emergency Management Department. Each department formally maintains and communicates mission-critical systems and disaster recovery protocols through each department's annual Department Emergency & Continuity of Operations Plan (DECOOP).
- **City Employees and Contractors:** Employees are the first line of defense in protecting systems from intruders. Per Personnel & ITA policies, every employee has a direct responsibility to protect City data and systems from disruption, act ethically, and report potential security issues early.

ENFORCEMENT ACROSS DEPARTMENTS AND THIRD-PARTY SYSTEMS

To maintain a secure environment, the City strictly enforces its cybersecurity policies through technical controls, Internal Enforcement (audits), and contractual obligations.

Technical Controls & Vulnerability Scanning

- **Vulnerability Scans:** The City mandates that departments weekly test their systems, servers, and websites to identify and mitigate any cyber threats. The ITA offers this service to City departments.
- **Patch Management:** Threats identified during these scans are categorized by severity (Critical, High, Medium, Low), and patches are applied to endpoints within strictly enforced timelines to ensure systems remain protected.

Internal Enforcement

- **Disciplinary Action:** The City takes security violations seriously. Policy violations by employees may result in disciplinary action up to and including discharge.
- **Ongoing Monitoring:** The City maintains the right to potentially monitor electronic information using City software or equipment, internet usage, and email patterns to ensure compliance with the law and City policy.

Third-Party and Vendor Enforcement

- **Vendor Vetting and Compliance:** The City actively vets prospective and current vendors to ensure their security practices align with recognized industry risk management standards.
- **Contractual Oversight:** Vendor agreements include established provisions for ongoing security assessments, ensuring that any required network access is securely managed and strictly limited to authorized City business.
- **Legal Action:** If a security policy violator is not a City employee, the matter is submitted to the Office of the City Attorney, who may refer the issue to law enforcement to consider criminal charges.

COMPLIANCE WITH CYBERSECURITY TRAINING AND LIABILITY PREVENTION

Human error is recognized as a significant threat to information security. The City actively mitigates this risk through mandatory education, fostering a culture of cybersecurity awareness.

- **Information Security Awareness Program:** The ITA maintains a comprehensive awareness program that mandates information security education for employees upon hire or when their work responsibilities change.
- **Annual Refreshers and Acknowledgments:** Employees are scheduled for "refresher" training on an annual basis. Furthermore, each applicable teammate must provide an annual signed acknowledgment confirming their understanding of and commitment to the Information Security Policies.
- **Preventing Future Liabilities:** The City's Risk Management Program is explicitly designed to prevent and minimize the risk of liability, protecting the financial, human, and tangible assets of the City. By facilitating staff participation in security awareness programs and actively promoting a culture of safety, the City reduces the probability of employees unknowingly disclosing sensitive information, thereby shielding the City from regulatory fines, reputational injury, and civil lawsuits.

Respectfully Submitted,

Ted Ross
General Manager

ec: Sharon Tso, Office of the Chief Legislative Analyst
Matt Szabo, City Administrative Officer
Melissa Velasco, City Administrative Officer
Robert Roth, City Administrative Officer
Austin Patrick, City Administrative Officer
ITA Executive Team