CITY OF CUPERTINO

**INNOVATION & TECHNOLOGY**

CITY HALL
10300 TORRE AVENUE • CUPERTINO, CA 95014-3255
TELEPHONE: (408) 777-3403 • FAX: (408) 777-3366
CUPERTINO.GOV

**CITY COUNCIL INFORMATIONAL MEMORANDUM**

Date: February 13, 2026

To: Cupertino City Council
From: Teri Gerhardt, CGCIO, Chief Technology Officer

Re: Regional Virtual Chief Information Security Officer (vCISO) Initiative

Background

Cybersecurity has become a core operational risk for local governments. The current threat landscape extends well beyond nuisance phishing emails or isolated system outages and now includes ransomware, supply-chain attacks, AI-driven fraud, data exfiltration, and increasing regulatory and audit scrutiny. Effectively managing these risks requires sustained, executive-level cybersecurity leadership focused on governance, strategy, and risk management—not solely technical tools or reactive consulting services.

In larger organizations, this role is typically fulfilled by a full-time Chief Information Security Officer (CISO). For a city of Cupertino's size, however, a full-time CISO is financially impractical, despite the City's cybersecurity risk profile increasingly resembling that of much larger organizations. As a result, many mid-sized cities face a structural gap: modern cybersecurity tools are in place, but without consistent executive-level oversight, long-term strategy, or coordinated governance.

To address this challenge, the Chief Information Officers of Cupertino, Palo Alto, Sunnyvale, and Mountain View propose procuring shared services through a regional virtual Chief Information Security Officer (vCISO) model.

*What a vCISO Provides*

A vCISO delivers the same executive-level cybersecurity leadership as an in-house CISO, but on a fractional, shared basis. The role emphasizes strategy, governance, compliance, and advisory support rather than day-to-day technical operations. Under this model, the vCISO would work directly with City leadership and IT staff to:

- Develop and maintain cybersecurity policies and protocols aligned with the NIST framework, including guidance on the responsible use of Artificial Intelligence

- Provide governance guidance and participate in strategic decision-making as needed
- Support internal and external cybersecurity audits and assessments
- Review new technologies, vendors, and contracts through a cybersecurity risk lens
- Provide ongoing thought leadership on emerging threats and best practices
- Serve as a surge resource during cybersecurity incidents or breaches

This approach strengthens the City's cybersecurity posture proactively, reducing reliance on reactive responses after incidents occur.

*An Innovative Regional Model*

The proposed regional vCISO model is innovative and, to staff's knowledge, has not been implemented in this form among peer cities. Rather than each city independently attempting to fund and retain senior cybersecurity leadership, this model leverages regional collaboration to address shared risks more effectively.

By pooling resources across jurisdictions, participating cities gain access to consistent, high-level cybersecurity leadership that would otherwise be unattainable individually. This represents a shift from isolated, city-by-city risk management toward a coordinated regional defense model—more closely aligned with how modern cyber threats operate across interconnected systems and vendors.

*Why a Regional Model Makes Sense*

The proposed vCISO would be shared across four cities that are similar in size, geography, and technical environment, and that already rely on many of the same cybersecurity tools, applications, and vendors. Because of these similarities, much of the cybersecurity work required is overlapping and reusable. Through shared services, the regional vCISO can:

- Develop common policies and governance artifacts once, rather than duplicating efforts in each city
- Conduct vendor and technology risk reviews that benefit all participating cities
- Standardize incident response planning and audit preparation
- Share insights, lessons learned, and best practices across jurisdictions

This approach reduces duplication of effort, improves consistency, and maximizes the value of existing cybersecurity investments.

*Cost and Value Considerations*

Following a review of proposals, the cities received quotes for vCISO services exceeding $100,000 annually. Through a regional evaluation of vendors, the Cities identified a reputable firm with a strong vCISO core practice that is willing to provide services at a cost of $45,000 per city, in partnership with Palo Alto, Sunnyvale, and Mountain View. All participating cities have identified funding within their FY 2026 budgets to move forward with this one-year pilot initiative before the end of the fiscal year. With the City Manager approval, Cupertino will also utilize infrastructure budget savings to support participation in the regional effort. Additionally, the vendor is an approved NASPO vendor, allowing the Cities to expedite the procurement process.

This shared model provides access to senior cybersecurity expertise that the City could not reasonably afford on its own, while maintaining fiscal responsibility. More importantly, it

enables a shift from a tool-centric, reactive cybersecurity posture to a strategic, governance-driven model better suited to the scale and persistence of today's cyber threats.

*Conclusion*
This initiative is not about adding another layer of bureaucracy. It is about modernizing how local governments protect critical systems, sensitive data, and public trust through collaboration, shared leadership, and a forward-looking approach to cybersecurity resilience. As cyber threats continue to grow in frequency, sophistication, and impact, the regional vCISO model allows participating cities to move forward together—strengthening both individual cybersecurity programs and the overall resilience of the region. The Technology, Information and Communication Commission (TICC) has been briefed on this proposal and is in full support of the initiative.

Fiscal Impact
The cost for the first year is $45K from each City for a multi-city contract with the consultant. However, sufficient funds are available within the Infrastructure Division budget to support this initiative. A budget proposal will be submitted for Fiscal Year 2027 to ensure continued funding, contingent upon the City realizing the anticipated value of the one-year pilot project.

City Work Program (CWP) Item/Description
None

Council Goal:
Quality of Life

California Environmental Quality Act
No California Environmental Quality Act impact.

---

Prepared by: Teri Gerhardt, CGCIO, Chief Technology Officer
Reviewed by: Floy Andrews, Interim City Attorney
Approved for Submission by: Tina Kapoor, City Manager