CITY OF SAN JOSE
CAPITAL OF SILICON VALLEY

Memorandum

TO: HONORABLE MAYOR AND CITY COUNCIL

FROM: Maria Öberg

SUBJECT: **See Below**

DATE: September 29, 2025

Approved

Date: 9/30/2025

COUNCIL DISTRICT: Citywide

SUBJECT: Amendments to Contract Awards for As-Needed Cybersecurity Products and Services

RECOMMENDATION

Adopt a resolution authorizing the City Manager or her designee to:

(a) Negotiate and execute the First Amendment with Adaptable Security Corp. (San José, CA), the Second Amendment with Illumant (Palo Alto, CA), and the First Amendment with MGT of America Consulting, LLC. (Tampa, FL), for various cybersecurity services to extend the terms of the Agreements for an additional five years through November 30, 2030, under the same material terms and conditions as the original Agreements, subject to the appropriation of funds;
(b) Negotiate and execute the Second Amendment with Spirent Communications (San José, CA) for cybersecurity services to extend the term of the Agreement for an additional five years through November 30, 2030, under the same material terms and conditions as the original Agreement, and to increase compensation by $125,820 for a revised maximum compensation of $525,820, subject to the appropriation of funds;
(c) Negotiate and execute the Second Amendment with NuHarbor Security Inc. (Colchester, VT) for cybersecurity services and tools to retroactively add two one-year options to extend the term of the Agreement through September 30, 2027, under the same material terms and conditions as the original Agreement, subject to the appropriation of funds;
(d) Negotiate and execute the First Amendment with Fortra Inc. (formerly Terranova Worldwide Corporation) (Quebec, Canada) for cybersecurity end user testing and training to add one one-year option to extend the term of the Agreement through March 31, 2027, under the same material terms and conditions as the original Agreement, subject to the appropriation of funds;

(e) Negotiate and execute the First Amendment with Second Renaissance Inc. (Olney, MD) for as required firewall management services to extend the term of the Agreement for an additional five years through March 31, 2031, under the same material terms and conditions as the original Agreement, subject to the appropriation of funds;
(f) Negotiate and execute the Second Amendment with Second Renaissance Inc. (Olney, MD) for as required supplemental advanced cybersecurity services to extend the term of the Agreement for an additional five years through June 30, 2030, under the same material terms and conditions as the original Agreement, and to increase compensation by $500,000 for a revised maximum compensation of $1,400,000, subject to the appropriation of funds; and
(g) Negotiate and execute the Fourth Amendment with Spruce Technology, Inc. (Clifton, NJ), and the Third Amendment with Insight Public Sector, Inc. (Herndon, VA) for as required supplemental advanced cybersecurity services to retroactively extend the term of the Agreements for an additional five years through June 30, 2030, under the same material terms and conditions as the Agreements, subject to the appropriation of funds.

SUMMARY AND OUTCOME

This memorandum provides the City Council with recommended actions that will allow the City Manager or her designee to negotiate and execute amendments to extend the terms of agreements with multiple vendors to continue providing the City of San José (City) with access to products and services to support and manage a strong cybersecurity program, spanning the National Institute of Standards and Technology Cybersecurity Framework program areas of risk identification, protection, detection, response, and recovery.

BACKGROUND

The City initiated its Cybersecurity Office, in the Information Technology Department, in 2018, with the mission of securing the City's information and systems from cybersecurity threats. This mission spans legal compliance requirements, professional management of technology assets and data, as well as work across City departments and the vendor community to ensure that cybersecurity is prioritized in both operations and projects. The City uses the National Institute of Standards and Technology Cybersecurity Framework and Special Publication 800-series in administering its cybersecurity program and protocols.

Cybersecurity risk is still an ongoing and elevated concern for public and private sector organizations. Given that level of concern, it is important for the City to: 1) acquire access to a robust and complementary set of cybersecurity products, services, and vendor-partners with which the City can prepare and manage security events in

advance, and 2) team with peer agencies to create an ecosystem of cybersecurity solutions and cooperative efforts that increase the baseline of cybersecurity for all communities, including intelligence sharing and joint response to cybersecurity events.

The cybersecurity-related contracts, originally awarded through the request for proposals, are now approaching the end of their terms. While staff intends to conduct a competitive solicitation for a new set of agreements for these cybersecurity services, at this time, staff do not think that the current environment is optimal for conducting the solicitation. To ensure continuity of service and to maintain the momentum on key cybersecurity initiatives, staff recommends extending the terms and, in some cases, increasing the compensation on these agreements. These extensions will allow the City to continue leveraging the deep institutional knowledge and trusted performance of current vendors while avoiding the operational and financial disruptions that may result from transitioning to new providers.

ANALYSIS

Extending the existing cybersecurity service contracts provides the most efficient and secure path forward to support the City's ongoing cybersecurity program. Several key considerations support this approach:

- **Continuity of Service and Risk Reduction**: Current vendors have an in-depth understanding of the City's technical environment and internal processes. Replacing them at this juncture would introduce onboarding delays, increased risk of service disruption, and potential knowledge gaps at a time when uninterrupted cybersecurity services are essential.
- **Proven Performance and Trust**: Each of the vendors have established a good working relationship with City departments. These working relationships would contribute directly to faster resolution times and reduced risk exposure.
- **Strategic Alignment**: The existing vendors have tailored their services to fit the City's specific cybersecurity needs and long-term goals. Their continued involvement supports strategic continuity and allows the City to build on progress already made.

EVALUATION AND FOLLOW-UP

This memorandum will not require any follow-up from staff.

COST SUMMARY/IMPLICATIONS

The recommended contract amendments include compensation increases for the Second Renaissance Inc. contract ($500,000) and the Spirent Communications contract

($125,820) to ensure adequate funding for ongoing cybersecurity services. Additionally, the other contracts are exercising options to be extended for years beyond 2025-2026. The total anticipated cost for cybersecurity services in 2025-2026 is $713,882 and will be funded by the General Fund, with the remaining amount for each of the contracts subject to the appropriation of funds.

1. TOTAL COST OF CONTRACTS

   A. Master Consultant Agreement with Spirent Communications for as required information systems security assessment services:

TOTAL COST OF CONTRACT/AGREEMENT	$400,000
Recommended Amendment Increase (as included in the memorandum)	125,820
TOTAL CONTRACT/AGREEMENT AMOUNT	**$525,820**

   B. Master Consultant Agreement with Second Renaissance Inc. for as required supplemental advanced cybersecurity services:

TOTAL COST OF CONTRACT/AGREEMENT	$900,000
Recommended Amendment Increase (as included in the memorandum)	500,000
TOTAL CONTRACT/AGREEMENT AMOUNT	**$1,400,000**

BUDGET REFERENCE

The table below identifies the fund and appropriation to fund the contracts recommended as part of this memorandum. The remaining funding is available for additional services citywide and subject to the appropriation of funds.

Fund #	Appn. #	Appropriation Name	Total Appropriation	Amount for Contract	2025-2026 Proposed Operating Budget Page*	Last Budget Action (Date, Ord. No.)
001	0432	Non-Personal / Equipment	$14,139,255	$713,882	591	6/17/2025 31230

** The 2025-2026 Adopted Operating Budget was approved on June 10, 2025 and adopted on June 17, 2025 by the City Council.*

COORDINATION

This memorandum has been coordinated with the City Attorney's Office, the City Manager's Budget Office, and the Information Technology Department.

PUBLIC OUTREACH

This memorandum will be posted on the City's Council Agenda website for the October 21, 2025 City Council meeting.

COMMISSION RECOMMENDATION AND INPUT

No commission recommendation or input is associated with this action.

CEQA

Not a Project, File No. PP17- 003, Agreements/Contracts (New or Amended) resulting in no physical changes to the environment.

PUBLIC SUBSIDY REPORTING

This item does not include a public subsidy as defined in section 53083 or 53083.1 of the California Government Code or the City's Open Government Resolution.

/s/
Maria Öberg
Director, Finance Department

For procurement and contract related questions, please contact Albie Udom, Deputy Director of Finance Department, Purchasing and Risk Management, at albie.udom@sanjoseca.gov.

For program related questions, please contact Auston Davis, City Information Security Officer, Information Technology Department, at auston.davis@sanjoseca.gov.