COUNCIL AGENDA: 2/23/21
FILE: 21-313
ITEM: 2.12

CITY OF SAN JOSE
CAPITAL OF SILICON VALLEY

Memorandum

TO: HONORABLE MAYOR AND CITY COUNCIL

FROM: Julia H. Cooper
Rob Lloyd

SUBJECT: SEE BELOW

DATE: February 1, 2021

Approved  Date 02/12/21

SUBJECT: REPORT ON REQUEST FOR PROPOSALS FOR AS-NEEDED CYBERSECURITY PRODUCTS AND SERVICES

RECOMMENDATION

Accept the report on the Request for Proposals and adopt a resolution authorizing the City Manager to:

(a) Negotiate and execute agreements with Adaptable Security Corp. (San José, CA), Illumant (Palo Alto, CA), MGT Consulting Group (Tampa, FL), and RSI Security (San Diego, CA) for as required information systems security assessment services (**Package A**) through November 30, 2025 and a maximum aggregate compensation not to exceed $1,600,000, subject to the appropriation of funds;

(b) Negotiate and execute amendments to agreements with Spirent Communications (San José, CA) and Tevora Business Solutions, Inc. (Irvine, CA) for as required information systems security assessment services (**Package A**) through November 30, 2025 to increase compensation by $80,000 for each agreement for an aggregate maximum compensation not to exceed $800,000, subject to the appropriation of funds;

(c) Negotiate and execute an amendment to the agreement with NuHarbor Security Inc. (Colchester, VT) for virtual security operations center services and tools (**Package B**) to add an additional nine months of services to cover the full initial term ending September 30, 2021, add four one-year options to extend the agreement through September 20, 2025 for ongoing services, software subscriptions, maintenance, and support, and increase compensation by $126,000 for a maximum compensation not to exceed $434,280 during the initial term, subject to the appropriation of funds;

(d) Negotiate and execute an agreement with Terranova Security (Quebec, Canada) for cybersecurity end user testing and training (**Package C**) for an initial one-year term ending March 31, 2022 and four one-year options to extend the agreement through March 31, 2026

for a maximum compensation not to exceed $35,000 during the initial one-year term, subject to the appropriation of funds;

(e) Negotiate and execute an agreement with Second Renaissance Inc. (Olney, MD) for as required firewall management services (**Package E**) through March 31, 2026 and a maximum compensation not to exceed $550,000, subject to the appropriation of funds;

(f) Negotiate and execute an agreement with Insight Public Sector (Herndon, VA) for advanced threat protection (**Package F**) for an initial one-year term ending March 31, 2022 and four one-year options to extend the agreement through March 31, 2026 for a maximum compensation not to exceed $95,468 during the initial one-year term, subject to the appropriation of funds;

(g) Negotiate and execute agreements with Global Solutions Group (Oak Park, MI), Stealth-ISS Group® Inc. (Arlington, VA), and Second Renaissance (Olney, MD) for as required supplemental advanced cybersecurity services (**Package G**) through June 30, 2025 and a maximum aggregate compensation not to exceed $1,500,000, subject to the appropriation of funds;

(h) Negotiate and execute amendments to agreements with Spruce Technology, Inc. (Clifton, NJ) and Insight Public Sector, Inc. (Herndon, VA) for as required supplemental advanced cybersecurity services (**Package G**) through June 30, 2025 to increase compensation by $180,000 each agreement for a maximum aggregate compensation not to exceed $1,000,000, subject to the appropriation of funds; and

(i) Negotiate and execute amendments and change orders for all agreements as required to address changes in the City's cybersecurity needs and reallocate funding between providers within each Package, consistent with the procurement and the City's standard terms and conditions, subject to the appropriation of funds.

OUTCOME

Provide the 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.

EXECUTIVE SUMMARY

Cybersecurity risks continue to grow in occurrence and impact for all organizations. Given that City of San José services span seven Critical Infrastructure Sectors as defined by the U.S. Cybersecurity and Infrastructure Security Agency, the City's approach to cybersecurity is two-fold: (1) acquire access to a robust and complementary set of cybersecurity products, services, and

vendor-partners that help the City prepare for security events in advance, and (2) team with peer agencies to select and use the ecosystem of cybersecurity solutions to increase the baseline of cybersecurity for all local governments.

To meet those goals, the Finance Department, on behalf of the Information Technology Department-Cybersecurity Office, conducted a large, multi-package procurement for As-Needed Cybersecurity Products and Services in FY 2019-2020. Review of proposals and selection of service providers was completed by a multi-jurisdiction team of large local governments, with the City of San José serving as the lead agency. This was a regional collaboration that allows other public agencies to leverage the procurement at their sole liability for contracting purposes, subject to their own procurement and contracting rules.

As a result of the procurement, staff recommends award of contracts to multiple vendors for six of the seven packages for City purposes. For these six packages, staff requests authority to negotiate and execute ten new agreements and amend five existing agreements that were executed under the City Manager authority to meet immediate needs. In addition, the multijurisdictional evaluation team pre-qualified additional vendors, so other agencies may utilize them based on their own procurement and contracting rules.

With these products, services, and vendor-partners in place, the City will have the tools to manage current and emerging cybersecurity risks. While recent exploits in the press make it clear that no organization is immune to cybersecurity incidents, these contract awards position the City to manage threats and vulnerabilities as effectively as possible. In tandem with efforts in business resilience and emergency management, staff aims to keep cybersecurity incidences few and their impacts minimal.

BACKGROUND

The City of San José 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 (NIST) Cybersecurity Framework (CSF) and Special Publication 800-series in administering its cybersecurity program and protocols. The NIST CSF was a product of Presidential Executive Order (EO) 13636, *Improving Critical Infrastructure Cybersecurity*, issued in February 2013 based on the recognition that the nation depends on the reliability and resilience of technology in the functioning of critical infrastructure. The Cybersecurity Enhancement Act of 2014[1] reinforced NIST's role in guiding protective cybersecurity standards, guidelines, and practices.

[1] Text - S.1353 - 113th Congress (2013-2014): Cybersecurity Enhancement Act of 2014 | Congress.gov | Library of Congress

The City's management of its cybersecurity risks affects its welfare in two primary ways: (1) direct impact through harm caused if life/safety/financial operations are compromised due to a breach, e.g., water/wastewater, aviation, traffic, financials, etc. and (2) indirect impact through the costs of impaired confidence in the City's management as determined through cybersecurity risks assessed in annual financial audits, reported in public debt offering statements, and in insurance reviews. Investments in cybersecurity and resilience maximize the City's ability to avoid harm and maintain the trust of its partners. Cybersecurity breaches in San Francisco (2016), Sacramento (2017), Atlanta (2018), Baltimore (2018 and 2019), and 20+ cities in Texas in coordinated fashion (2019) demonstrated that local governments face tens of millions of dollars in direct response and recovery costs, along with other potential ancillary impacts, if they are the victim of a major breach and are unprepared. These facts elevated the priority of cybersecurity procurement for the Information Technology and Finance Departments.

It is important to note that cybersecurity risks continue to grow in occurrence and impact for all organizations. An average of two local/tribal governments report a major service outage, systems breach, or data exfiltration event per week. Given that City services span seven Critical Infrastructure Sectors as defined by the U.S. Cybersecurity and Infrastructure Security Agency (CISA), San José imperatives are 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.

A strong cybersecurity program requires a capable team, rigorous processes, and effective technology tools. Aligning with the NIST CSF functions of Identify, Protect, Detect, Respond, and Recover, the City cybersecurity approach creates capabilities that integrate tools and practices into citywide operations to significantly improve the City's risk profile. The approach used in this Request for Proposals (RFP) supports those goals and forms the essential cybersecurity toolbox for operational needs and crisis response.

ANALYSIS

In May 2019, the Finance Department released a Request for Proposals (RFP) for As-Needed Cybersecurity Products and Services through its e-procurement system. The RFP was divided into seven packages:

- Package A – Information Systems Security Assessment Services
- Package B – Virtual Security Operations Center (VSOC) Services and Tools
- Package C – Cybersecurity End User Training and Testing
- Package D – Incident Response – Legal, Media, and Cyber Forensic Guidance Services and Tools
- Package E – Firewall Management Services
- Package F – Advanced Threat Protection Services and Tools
- Package G – Supplemental Advanced Cybersecurity Services

Each package included a unique scope of services, and proposers could submit proposals for any or all the packages. A total of 253 companies viewed the RFP, and 50 companies submitted proposal responses prior to the submittal deadline for the six packages included in this recommendation. Since each vendor could submit proposals for multiple packages, there were a total of 125 proposal responses evaluated for these six packages. See Appendix 1 for a list of vendor responses by package, excluding Package D which is not included in this Council action.

Evaluation Process: Proposals were evaluated and scored independently, in accordance with the evaluation criteria set forth in the RFP, by a four-member evaluation team comprised of cybersecurity and technology leaders from the City Information Technology Department, the City and County of San Francisco, and the County of Santa Clara. Evaluations were conducted in phases with Phase 1 evaluations focused on experience and qualifications and Phase 2 evaluations focused on technical capabilities and incorporating cost. Only vendors scoring in the competitive range on their Phase 1 evaluations moved forward to Phase 2. Final evaluation results by package are summarized below.

Package A – Information Systems Security Assessment Services

Package A included a scope of services for as-needed information systems security assessments, which are audits and reviews of the City's information systems security processes, practices, and overall security readiness. The City received 29 responsive written proposals for this package by the RFP deadline. Sixteen proposers were selected to move forward for Phase 2 evaluations based on their Phase 1 scores, and seven finalists were selected to participate in a Best and Final Offer (BAFO) based on their Phase 2 scores. Scores for the finalists are as follows:

Final Scores	**Maximum Points**	**Spirent Communications**	**Accenture***	**Tevora Business Solutions, Inc.**	**Adaptable Security Corp**	**Illumant**	**MGT Consulting Group**	**RSI Security**
Experience and Qualifications	35	29	31	32	27	32	32	27
Technical Capabilities	40	25	30	30	25	22	27	21
BAFO Cost	15	15	1	4	2	10	4	11
Local Business Preference	5	0	5	0	5	0	0	0
Small Business Preference	5	0	0	0	5	0	0	0
TOTAL	**100**	**69**	**67**	**66**	**64**	**64**	**63**	**59**

*Vendor submitted exceptions to City's standard terms, and the City was unable to reach agreement with the vendor. Therefore, no award of contract is being made.

This package requires multiple contracts for these as-needed services, so staff recommends award of contract to all finalists, excluding Accenture. Contracts with Spirent Communications and Tevora Business Solutions, Inc. were executed under the City Manager's contract authority to

address immediate City needs while the evaluation process was being completed for all packages. Additionally, all finalists, including Accenture, were prequalified through this process for other public entities to leverage, at their sole liability, for contracting purposes based on their own procurement and contracting rules. All vendors were confirmed to have no active exclusions on the Federal government's contract award management system, www.sam.gov, prior to issuing the Notice of Intended Award.

Package B – Virtual Security Operations Center (VSOC) Services and Tools

Package B included a scope of services for 24x7x365 monitoring services of City IT assets such as websites, applications, databases, data centers, servers, networks, desktops, and other endpoints to help the City prevent, protect, and recover from malicious threats and attacks to the City infrastructure and applications. The City received 22 responsive written proposals for this package by the RFP deadline. Eight proposers scored in the competitive range based on their Phase 1 scores and moved forward for Phase 2 evaluation. The two highest scoring vendors following Phase 2 evaluations participated in oral interviews/system demonstrations and a Best and Final Offer (BAFO). Scores for the finalists are as follows:

Final Scores	Maximum Points	NuHarbor Security	FireEye, Inc.
Experience and Qualifications	35	28	25
Technical Capabilities	40	29	34
BAFO Cost	15	15	6
Local Business Preference	5	0	0
Small Business Preference	5	0	0
TOTAL	**100**	**72**	**65**

To address the City's immediate need for these services, an agreement was executed with NuHarbor Security under the City Manager's contract authority while the evaluation process was being completed for all packages. Additionally, both finalists were prequalified through this process for other public entities to leverage either, at their sole liability, for contracting purposes based on their own procurement and contracting rules. Reference checks were conducted, and staff verified there were no active exclusions on www.sam.gov for both vendors prior to issuing the Notice of Intended Award.

Package C – Cybersecurity End User Testing and Training

Package C included a scope of services for the provision of resources and tools for tiered web-based training that provides end users with fundamental security knowledge such as phishing emails, password/passphrase best practices, social engineering, IT-related advanced security training, and compliance training. The City received 12 responsive responses for this package by the RFP deadline. Eight proposers scored in the competitive range based on their Phase 1 scores and moved forward for Phase 2 evaluation. The City then conducted a Best and Final Offer (BAFO) with the four highest scoring vendors following Phase 2 evaluations. Scores for the finalists are as follows:

Final Scores	Maximum Points	Terranova Security	Atos	AT&T Inc.	Insight Public Sector, Inc.
Experience and Qualifications	35	27	27	26	24
Technical Capabilities	40	30	33	30	32
BAFO Cost	15	15	10	12	2
Local Business Preference	5	0	0	0	5
Small Business Preference	5	0	0	0	0
TOTAL	**100**	**72**	**70**	**68**	**63**

Based on these results, staff recommends award of contract to Terranova Security as the best value vendor. Additionally, all finalists were prequalified through this process for other public entities to leverage, at their sole liability, for contracting purposes based on their own procurement and contracting rules. All vendors were confirmed to have no active exclusions on www.sam.gov prior to issuing the Notice of Intended Award.

Package D – Incident Response

No recommendation of award is being made for this package at this time. Staff will return to Council with a recommendation for these services at a later date.

Package E – Firewall Management Services

Package E included a scope of services for firewall management services to provide the City with supplemental firewall management expertise to achieve maximum security, awareness, and automation at the City's network perimeter. The City received 12 responsive written proposals for this package by the RFP deadline. Five proposers scored in the competitive range based on their Phase 1 scores and moved forward for Phase 2 evaluation and a Best and Final Offer (BAFO). Three finalists withdrew themselves from further consideration during the BAFO process. Scores for the remaining finalists are as follows:

Final Scores	Maximum Points	Second Renaissance Inc.	EVOTEK, Inc.
Experience and Qualifications	35	24	20
Technical Capabilities	40	24	24
Cost (BAFO)	15	15	10
Local Business Preference	5	0	0
Small Business Preference	5	0	0
TOTAL	**100**	**63**	**54**

Based on these results, staff recommends award of contract to Second Renaissance Inc. as the best value vendor. Additionally, both finalists were prequalified through this process for other public entities to leverage, at their sole liability, for contracting purposes based on their own procurement and contracting rules. All vendors were confirmed to have no active exclusions on www.sam.gov and reference checks were conducted for Second Renaissance prior to issuing the Notice of Intended Award.

Package F – Advanced Threat Protection Services and Tools

Package F included a scope of services for advanced threat protection services and tools to provide the City with protection again known, unknown, and zero-day threats. The City received 28 written proposals for this package by the RFP deadline; one proposal was deemed non-responsive and removed from further consideration. Ten proposers scored in the competitive range based on their Phase 1 scores and moved forward for Phase 2 evaluation. The four highest scoring vendors following Phase 2 evaluations moved forward for oral interviews/system demonstrations and a Best and Final Offer (BAFO). Scores for the finalists are as follows:

Final Scores	Maximum Points	Insight Public Sector	ComputerLand Silicon Valley	NuHarbor Security	Presidio Networked Solutions
Experience and Qualifications	35	24.79	26.83	27.13	27.42
Technical Capabilities	40	31.25	29.50	33.25	29.00
BAFO Cost	15	15.00	9.20	7.56	6.52
Local Business Preference	5	5.00	5.00	0.00	0.00
Small Business Preference	5	0.00	5.00	0.00	0.00
TOTAL	**100**	**76.04**	**75.53**	**67.94**	**62.94**

Based on these results, staff recommends award of contract to Insight Public Sector as the best value vendor. Additionally, all finalists were prequalified through this process for other public entities to leverage, at their sole liability, for contracting purposes based on their own procurement and contracting rules. All vendors were confirmed to have no active exclusions on www.sam.gov prior to issuing the Notice of Intended Award.

Package G – Supplemental Advanced Cybersecurity Services

Package G provided a scope of services for supplemental advanced cybersecurity services for projects, tasks, and/or supplemental staffing as required. The City received 23 responsive written proposals for this package by the RFP deadline. Thirteen proposers scored in the competitive range based on their Phase 1 scores and moved forward for Phase 2 evaluations. Eight finalists were invited to participate in a BAFO based on their Phase 2 scores. Two of the finalists were disqualified during the BAFO round, one for excessive exceptions to the City standard terms and conditions and the other for failing to submit a BAFO response. Scores for the remaining finalists are as follows:

Final Scores	**Maximum Points**	**Insight Public Sector**	**Spruce Technology, Inc.**	**Global Solutions Group**	**Stealth ISS Group**	**Accenture***	**Second Renaissance**
Experience and Qualifications	35	26	25	26	24	27	31
Technical Capabilities	40	27	30	24	29	32	21
Cost (BAFO)	15	8	11	15	12	0	10
Local Business Preference	5	5	0	0	0	5	0
Small Business Preference	5	0	0	0	0	0	0
TOTAL	**100**	**66**	**66**	**65**	**65**	**64**	**62**

*Vendor submitted exceptions to the City standard terms and conditions, and the City was unable to reach agreement with the vendor. Therefore, no award of contract is being made.

This package requires multiple contracts for these as-needed services, so staff recommends award of contract to all finalists, excluding Accenture. Contracts with Insight Public Sector and Spruce Technology, Inc. were executed under the City Manager contract authority to address immediate City needs while the evaluation process was being completed for all packages. Additionally, all finalists, including Accenture, were prequalified through this process for other public entities to leverage, at their sole liability, for contracting purposes based on their own procurement and contracting rules. All vendors were confirmed to have no active exclusions on www.sam.gov prior to issuing the Notice of Intended Award.

Local and Small Business Enterprise Preference: In accordance with City policy, ten percent of the total evaluation points were reserved for local and small business preference. Multiple vendors requested and received the local and small business preference for their offices located within Santa Clara County as noted in the result summaries above.

Protest: The City RFP process included a ten-day protest period that began when the City issued the Notice of Intended Award for each package. No protests were received.

Award Recommendations: See next page.

STAFF RECOMMENDS AWARDS OF CONTRACT TO THE VENDORS IDENTIFIED BELOW WHOSE PROPOSALS WERE SCORED AS THE BEST VALUE PROPOSALS PER THE EVALUATION CRITERIA SET FORTH IN THE RFP:

Vendor	Initial Term	One-Year Option Terms	Current Contract Amount	Requested Increase	Maximum Compensation (Initial Term)
Package A - Information Systems Security Assessment Services (as required)					
Adaptable Security Corp.	5 years	0	N/A	N/A	$400,000
Illumant	5 years	0	N/A	N/A	400,000
Mgt Consulting Group	5 years	0	N/A	N/A	400,000
RSI Security	5 years	0	N/A	N/A	400,000
Spirent Communications	5 years	0	$320,000	$80,000	400,000
Tevora Business Solutions, Inc.	5 years	0	$320,000	$80,000	400,000
Subtotal Package A - Recommendations (a) and (b)					**$2,400,000**
Package B - Virtual Security Operations Center Services and Tools					
NuHarbor Security Inc.	1 year	4	$308,280	$126,000	$434,280
Subtotal Package B - Recommendation (c)					**$434,280**
Package C - Cybersecurity End User Testing and Training					
Terranova Security	1 year	4	N/A	N/A	$35,000
Subtotal Package C - Recommendation (d)					**$35,000**
Package E – Firewall Management Services (as required)					
Second Renaissance Inc.	5 years	0	N/A	N/A	$550,000
Subtotal Package E – Recommendation (e)					**$550,000**
Package F – Advanced Threat Protection					
Insight Public Sector	1 year	4	N/A	N/A	$95,468
Subtotal Package F – Recommendation (f)					**$95,468**
Package G – Supplemental Advanced Cybersecurity Services (as required)					
Global Solutions Group	5 years	0	N/A	N/A	$500,000
Stealth-ISS Group® Inc.	5 years	0	N/A	N/A	500,000
Second Renaissance	5 years	0	N/A	N/A	500,000
Spruce Technology, Inc.	5 years	0	$320,000	$180,000	500,000
Insight Public Sector, Inc.	5 years	0	$320,000	$180,000	500,000
Subtotal Package G – Recommendations (g) and (h)					**$2,500,000**

GRAND TOTAL ALL PACKAGES INCLUDED IN THIS RECOMMENDATION (NOT TO EXCEED) **$6,014,748**

Summary of Agreements: All agreements with the recommended vendors will be in accordance with the City's standard terms and conditions and include the following provisions:

Packages A, E, and G:

1. Fixed not-to-exceed rates for a five-year term and a not-to-exceed amount for each agreement, with compensation based on actual services requested by the City (through executed service orders, subject to the appropriation of funds) and provided by the vendors; and
2. Detailed scopes of services to ensure that the services comply with the City's requirements.

Packages B, C, and F:

1. Fixed not-to-exceed rates with compensation based on actual services provided by the vendors;
2. Detailed scopes of services to ensure that the services comply with the City's requirements; and
3. One-year initial terms with four one-year options to extend the agreements.

CONCLUSION

Approval of this recommendation will ensure the City has access to the cybersecurity tools and services required to manage cybersecurity threats and vulnerabilities as effectively as possible. Few organizations have a broad array of products, services, and vendor-partners set in advance to both minimize risks and maximize response capabilities. The contractual capacities created by these contracts are large, but require appropriated funding, which is handled in the City Budget Process. Approval of this recommendation will provide the City one of the highest levels of coordinated coverage, while also positioning the City's work to help other local governments.

EVALUATION AND FOLLOW-UP

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

CLIMATE SMART SAN JOSE

The recommendation in this memorandum has no effect on Climate Smart San José energy, water, or mobility goals.

PUBLIC OUTREACH

This memorandum will be posted on the City Council Agenda website for the City of San José Council meeting to be held on February 23, 2021.

COORDINATION

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

COMMISSION RECOMMENDATION/INPUT

No commission recommendation or input is associated with this action.

FISCAL/POLICY ALIGNMENT

This action is consistent with the City Council-approved budget strategy to effectively manage the City's technology resources to enable and enhance the delivery of City Services and projects. It is consistent with priorities approved in the most recent IT Strategic Plan as well as the 2020-2021 City Roadmap, both approved by City Council.

COST SUMMARY/IMPLICATIONS

1. AMOUNT OF RECOMMENDATION (initial terms) $6,014,748

2. COST ELEMENTS:	**Not to Exceed**
Package A – Information Systems Security Assessments (as needed)	**(initial terms)**
Adaptable Security Corp. (5-year term)	$400,000
Illumant (5-year term)	400,000
Mgt Consulting Group (5-year term)	400,000
RSI Security (5-year term)	400,000
Spirent Communications (5-year term)	400,000
Tevora Business Solutions, Inc. (5-year term)	400,000
Package A Subtotal	**$2,400,000**
Package B – Virtual Security Operations Center Services and Tools	
NuHarbor Security, Inc. (initial 1-year term)	$434,280
Package B Subtotal	**$434,280**
Package C – Cybersecurity End User Testing and Training	
Terranova Security (initial 1-year term)	$35,000
Package C Subtotal	**$35,000**
Package E – Firewall Management Services (as needed)	
Second Renaissance, Inc. (5-year term)	$550,000
Package E Subtotal	**$550,000**
Package F – Advanced Threat Protection	
Insight Public Sector (initial 1-year term)	$95,468
Package F Subtotal	**$95,468**
Package G – Supplemental Advanced Cybersecurity Services (as needed)	

Global Solutions Group (5-year term)	$500,000
Stealth-ISS Group®, Inc. (5-year term)	500,000
Second Renaissance (5-year term)	500,000
Spruce Technology, Inc. (5-year term)	500,000
Insight Public Sector, Inc. (5-year term)	500,000
Package G Subtotal	**$2,500,000**
INITIAL TERMS NOT-TO-EXCEED (ALL CONTRACTS)	**$6,014,748**

3. SOURCE OF FUNDING:

Funding for cybersecurity-related products and services exists within the General Fund Information Technology Department Non-Personal/Equipment appropriation, with $1,399,000 included for 2020-2021. Options to be exercised after the current fiscal year are subject to the appropriation of funds through future budgeting cycles.

Packages B, C, and F include encumbered funds totaling $564,748 for the initial one-year terms, and option terms will be exercised subject to the appropriation of funds. Services to be utilized under the five-year contracts for Packages A, F, and G are for a currently undetermined quantity and value, and $834,252 is currently appropriated and will be used as needed. Packages A, F, and G are set up as master agreements with a not-to-exceed amount; work may only commence, and funds are certified and encumbered through the execution of service orders that draw down on the not-to-exceed amount. Required services beyond the current appropriation (but under the contract not-to-exceed amount), will be subject to the appropriation of funds.

The Administration will recommend the allocation of any additional funding as necessary to cost-effectively manage risks as assessed by the Cybersecurity Office.

4. FISCAL IMPACT: Subject to availability and approval of funding through the annual budget process.

BUDGET REFERENCE

The table below identifies the funds and appropriations to fund the contract recommended as part of this memorandum.

Fund #	Appn. #	Appn. Name	Total Appn.	Amt. for Contract	2020-2021 Adopted Operating Budget Page	Last Budget Action (Date, Ord. No.)
001	0432	Non-Personal/ Equipment – Information Technology	$10,325,301	$1,399,000	VIII – 249	10/20/2020, 30494

CEQA

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

/s/
ROB LLOYD
Chief Information Officer

/s/
JULIA H. COOPER
Director of Finance

For questions regarding the procurement, please contact Jennifer Cheng, Deputy Director of Finance, at jennifer.cheng@sanjoseca.gov. For questions regarding the City's cybersecurity program, please contact Marcelo Peredo, City Information Security Officer, at marcelo.peredo@sanjoseca.gov.

Attachment

Appendix 1
Proposal Responses by Package

Following are vendor responses by package received for the City's As-Needed Cybersecurity Products and Services RFP. The RFP included seven (7) packages: Package A – Information Systems Security Assessment Services, Package B – Virtual Security Operations Center (VSOC) Services and Tools, Package C – Cybersecurity End User Training and Testing, Package D – Incident Response – Legal, Media, and Cyber Forensic Guidance Services and Tools, Package E – Firewall Management Services, Package F – Advanced Threat Protection Services and Tools, and Package G – Supplemental Advanced Cybersecurity Services. A total of 125 proposal responses from fifty (50) vendors for the six (6) packages included in this recommendation were reviewed and scored by the evaluation panel.

Vendor	A Assessments	B VSOC	C Training	E Firewall	F Threat Prot.	G Supplemental
Accenture	✓	✓			✓	✓
Adaptable Security Corp.	✓					
AT&T	✓	✓	✓	✓	✓	✓
Atos	✓	✓	✓	✓	✓	✓
Axiado					✓	
Brownstone Consulting Firm	✓					✓
Business Telephone Exchange, Inc. (BTX)		✓			✓	
Carahsoft	✓	✓		✓	✓	
ComputerLand		✓			✓	
Dark Trace					✓	
Data Shield (RSA)		✓	✓		✓	✓
Digital Scepter					✓	
Evotek	✓	✓		✓	✓	✓
FireEye	✓	✓			✓	
FTI Consulting	✓					
Global Solutions Group	✓					✓
GLS		✓		✓		✓
Hacking Solutions	✓	✓	✓			✓
Hftech	✓	✓	✓	✓	✓	✓
Illumant	✓					
Insight Public Sector	✓		✓		✓	✓
Integrated Archive Systems					✓	
InterVision		✓			✓	✓
Ladlas Prince LLC	✓		✓			
Level 5 / Versiant / SEC Consult America	✓	✓	✓	✓	✓	✓
MGT Consulting Group	✓	✓	✓		✓	✓
NuHarbor Security Inc.	✓	✓			✓	✓
Ordr					✓	
Ping Identity					✓	
Plante Moran	✓					
Presidio Networked Solutions Group, LLC		✓			✓	
RSI Security	✓					✓
Second Renaissance Inc.	✓	✓	✓	✓		✓
Securance Consulting	✓					
Security Foundations US	✓	✓				
SentinelOne		✓			✓	

Vendor	A Assessments	B VSOC	C Training	E Firewall	F Threat Prot.	G Supplemental
Sharper Technology				✓	✓	
SHI International	✓				✓	
Six Degrees Consulting				✓	✓	
Skybox Security				✓		
Softworld/Pelta						✓
Spirent Communications	✓					
Spruce Technology, Inc.						✓
Stealth-ISS® Group Inc.	✓	✓				✓
StrongKey						✓
Tech Mahindra	✓	✓	✓	✓	✓	✓
Teranova Security			✓			
Tevora Business Solutions, Inc.	✓					
Thornton Tomasetti	✓					
Vectra AI, Inc.					✓	
COUNT	**29**	**22**	**12**	**12**	**28**	**22**

Note: Package D – Incident Response is not included in this Council action as a Notice of Intended Award has not yet been issued. Staff will return to Council with an award recommendation for these services at a later date.