Exhibit A
Master City of San José Consultant Agreement
Approved Service Order Form

(Non-Capital Projects)

Cover Page

1a. Intentionally Omitted **1b.** AC Contract No.: **AC 31754**

2. Approved **Service Order No. 4**

3. Consultant's Name: **Spirent Communications Inc.**

4. Project Name: Gray box/White box Penetration Testing – Detect Log4j Vulnerability

5. Project Location: All work performed remotely with a focused penetration test for Log4j on CSJ's internal servers/IPs.

6. The Consultant and the City will implement this Approved Service Order in accordance with the Master Agreement, this cover page and Attachments "A" (Tasks), "B" (Terms and Conditions), and "C" (Compensation Table), and Exhibit "D" (Schedule of Specific Services) which are incorporated herein by references.

7. Budget/Fiscal:

a. Current **unencumbered** amount in Master Agreement:	$	350, 440
b. **Maximum Service Order Compensation for this Approved Service Order:**	$	15,340
c. New unencumbered balance in Master Agreement (7.a – 7.b):	$	335, 100

d. **Appropriation Certification**: I certify that an unexpended appropriation in the amount of the Maximum Service Order Compensation is available in the following fund(s) and that such fund(s) will be encumbered to pay for this Approved Service Order.

Fund: 001 Appr Amount: $15,340

Devika Tandan
Email: devika.tandan@sanjoseca.gov

Authorized Signature: ______

8. **Division Analyst Approval:** Marcelo Peredo
Email: marcelo.peredo@sanjoseca.gov

9. **Consultant Approval:** Sameer Dixit
Email: sameer.dixit@spirent.com

10. **Approval as to Form (City Attorney):**

☒ Service Order Form Approved by the Office of the City Attorney
(Maximum Service Order Compensation is $100,000 or less, and the provisions of the service order form are not altered.)

☐ Approved as to Form: ______ Date: ______

11. **City Director Approval:** Vickie J. Davis
Email: vickie.davis@sanjoseca.gov

Attachment A: Tasks

The Consultant shall provide the services and deliverables set forth in this **Attachment A**. The Consultant shall provide all services and deliverables required by this **Attachment A** to the satisfaction of the City's contract manager.

General Description of Project for which Consultant will Provide Services: General Description of Project for which Consultant will Provide Services: Spirent will provide security audit/assessment services that are designed to gauge and demonstrate real-world vulnerability to current, authentic attacks. With a scope tailored to suit the system under test, these assessments reflect the multi-faceted challenges and realities of securing assets against modern, skilled adversaries. Spirent methodologies are aligned with well-known industry standards, including NIST, NSA-ISAM, CREST, PTES and OWASP guidelines.

Task No. 1:

A. <u>Services</u>: Gray Box Penetration Testing – Log4j Unauthenticated Scanning

<u>Overview:</u>

Spirent SecurityLabs White Box penetration test performs a thorough assessment of the in-scope target environment and outputs a detailed deliverable with both tactical & strategic recommendations to improve the security posture of the customer's infrastructure.

In this task, Spirent will focus on internal Log4j unauthenticated scanning on environments hosted at the City of San José agreed upon in-scope assets. Spirent will provide a virtual machine that is deployable into the environment under test, which will connect back to Spirent's command and control infrastructure. Consultants will then conduct testing through this VM to assess the effectiveness of network segmentation and surface any vulnerabilities that might be available to an attacker who gains a foothold in the internal environment.

Spirent SecurityLabs to focus the engagement on directed attack logic-based testing against the exploitation of the new vulnerability identified as CVE-2021-44228 affecting the java logging package, Log4j. This vulnerability has a severity score of 10.0, most critical designation, and offers remote code execution on hosts engaging with software that uses Log4j utility. This attack has also been called "Log4Shell".

The Emergency penetration testing project shall proceed in the following phases:

<u>Project Planning</u>:

- The internal network penetration test will be performed remotely.

<u>Assessment and Analysis:</u>

- Based on the external network penetration test conducted before the scheduled internal network assessment, Spirent consultants will start with understanding and mapping the internal network. The City of San José will ensure that Spirent consultants are whitelisted and permitted to evaluate the security posture of the in-scope assets with minimal impedances from Network Security Controls and IDS/IPS systems. Spirent consultants will proceed with the testing based on the agreed-upon scope and will immediately notify the City of San José's critical team members and stakeholders of any high/critical severity findings.
- While the exact activities within a penetration test will vary depending upon the technology used in the environment, engagements will generally adhere to the following approach:
  - Manual and Automated Vulnerability Scanning

□ Service Enumeration and Fingerprinting

□ Testing for Published Vulnerabilities and Misconfigurations:

1. Unauthenticated Scanning:
    a. Log4j and Java weaknesses concerning Log4j
    b. Validation thought non-impactful means
        i. Validation only, no active exploitation
    c. Log evidence and report weaknesses found to the Portal

□ Report debriefs and review of findings

B. <u>Deliverable</u>:

Spirent SecurityLabs shall deliver an assessment report that includes:

a. An executive summary that provides an overview of findings, and a high-level summary of key project activities.

b. The detailed findings describe the issue and its causes in-depth, identify affected assets, assign a severity level according to Spirent's rating scale, and recommendations to remediate or mitigate the vulnerability. The report also contains a detailed narrative, which outlines how vulnerabilities link together in the attack chain and provide insight into the evolution of a successful exploitation operation.

c. Walkthrough for findings and impact and remediation strategy

C. <u>Completion Time</u>: The Consultant must complete the services and deliverable for this task in accordance with whichever one of the following time is marked:

□ On or before the following date: ________________________________.

☒ On or before 30 Business Days from February 28, 2022.

Task No. 2:

A. <u>Services</u>: White Box Penetration Testing – Authenticated Scanning / Validation

<u>Overview:</u>

Spirent SecurityLabs White Box penetration test performs a thorough assessment of the in-scope target environment and outputs a detailed deliverable with both tactical & strategic recommendations to improve the security posture of the customer's infrastructure.

In this task, Spirent will focus on internal Log4j authenticated scanning/validation on environments hosted at the City of San José agreed upon in-scope assets. Spirent will provide a virtual machine that is deployable into the environment under test, which will connect back to Spirent's command and control infrastructure. Consultants will then conduct testing through this VM to assess the effectiveness of network segmentation and surface any vulnerabilities that might be available to an attacker who gains a foothold in the internal environment.

Spirent SecurityLabs to focus the engagement on directed attack logic-based testing against the exploitation of the new vulnerability identified as CVE-2021-44228 affecting the java logging package, Log4j. This vulnerability has a severity score of 10.0, most critical designation, and offers remote code execution on hosts engaging with software that uses Log4j utility. This attack has also been called "Log4Shell".

The Emergency penetration testing project shall proceed in the following phases:

<u>Project Planning</u>:

- The internal network penetration test will be performed remotely.

<u>Assessment and Analysis</u>:

- Based on the internal Log4j unauthenticated scanning conducted, Spirent consultants will start authenticated scanning/validation of the internal network. The City of San José will ensure that credentials are provided and Spirent consultants are whitelisted and permitted to evaluate the security posture of the in-scope assets with minimal impedances from Network Security Controls and IDS/IPS systems. Spirent consultants will proceed with the testing based on the agreed-upon scope and will immediately notify the City of San José's critical team members and stakeholders of any high/critical severity findings.

- Spirent will observe if any of these Indicators of Compromise (IoCs) concerning known Log4j attacks exists, however it is not a primary goal of this assessment. If any IoCs are observed while conducting the duties outlined in this SO, Spirent Consultants will notify critical team members and stakeholders but will no longer perform any actions against the specific systems in which IoCs are identified. This is to ensure the environment is as sanitary as possible and preserve the evidence for further evaluations by qualified professionals.

- While the exact activities within a penetration test will vary depending upon the technology used in the environment, engagements will generally adhere to the following approach:
  - Manual and Automated Vulnerability Scanning
  - Service Enumeration and Fingerprinting
  - Testing for Published Vulnerabilities and Misconfigurations:
    1. Authenticated Scanning / Validation
       a. Validate weaknesses concerning Log4j
       b. Validate other weaknesses concerning 3rd party Java Services
       c. Log evidence and report weaknesses found to the Portal
  - Report debriefs and review of findings

C. **Deliverable:**

Spirent SecurityLabs shall deliver an assessment report that includes:

a. An executive summary that provides an overview of findings, and a high-level summary of key project activities.

b. The detailed findings describe the issue and its causes in-depth, identify affected assets, assign a severity level according to Spirent's rating scale, and recommendations to remediate or mitigate the vulnerability. The report also contains a detailed narrative, which outlines how vulnerabilities link together in the attack chain and provide insight into the evolution of a successful exploitation operation.

c. Walkthrough for findings and impact and remediation strategy

C. Completion Time: The Consultant must complete the services and deliverable for this task in accordance with whichever one of the following time is marked:

□ On or before the following date: ________________________________.

☒ On or before 30 Business Days from February 28, 2022

Attachment B: Terms and Conditions

1. **City's Contract Manager:** The City's contract manager for this Approved Service Order is:

Name: Marcelo Peredo	Phone No.: 202-669-1672
Department: ITD	E-mail: marcelo.peredo@sanjoseca.gov
Address: 200 E. Santa Clara Street, San José, CA 95113	

2. **Consultant's Contract Manager and Other Staffing:** Identified below are the following: (a) the Consultant's contract manager for this Approved Service Order, and (b) the Consultant(s) and/or employee(s) of the Consultant who will be principally responsible for providing the services and deliverables. ***If an individual identified below does not have a current Form 700 on file with the City Clerk for a separate agreement with the City, and is required to file a Form 700, the Consultant must comply with the requirements of Subsection 17.2 of the Master Agreement, entitled "Filing Form 700."***

		Required to File Form 700?		
Consultant's Contract Manager		**Yes Already Filed (Date Filed)**	**Yes Need to File**	**No**
Name: Sameer Dixit	Phone No.: 408.752.7180			**X**
Address: 2709 Orchard Parkway, Suite 20, San José, CA 95134	E-mail: sameer.dixit@spirent.com			
Other Staffing				
Name:	Assignment:			
1. Tej Aulakh	Project Manager/Security Auditor			X

3. **<u>Subconsultants</u>:** Whichever of the following is marked applies to this Approved Service Order:

☒ The Consultant can ***not*** use any subconsultants.

□ The Consultant can use the following subconsultants to assist in providing the required services and deliverables:

<u>Subconsultant's Name</u>	**<u>Area of Work</u>**
1.	
2.	
3.	

4. **<u>Reimbursable Expenses</u>:** If the Compensation Table set forth in **Attachment C** of this Approved Service Order states that the City will reimburse the Consultant for expenses, then only the expenses identified in Subsection 10.5.3 of the Master Agreement are Reimbursable Expenses unless the following box is marked and additional reimbursable expenses are set forth:

□ In addition to the expenses identified in Subsection 10.5.3 of the Master Agreement, the following expenses are Reimbursable Expenses:

<u>Additional Reimbursable Expense(s)</u>	**<u>Mark-up</u>**
1. ____	________
2. ____	________
3. ____	_________

Notwithstanding the foregoing, any additional reimbursable expense(s) set forth in the above table will be disregarded if the Compensation Table states that the City will *not* reimburse the Consultant for any expenses.

Attachment C: Compensation Table

The City will compensate the Consultant for providing the services and deliverables set forth in **Attachment A** in accordance this Compensation Table. This Compensation Table is subject to the terms and conditions set forth in the Master Agreement, including without limitation Section 10 of the Master Agreement.

Part 1 – Compensation for Services and Deliverables			
Column 1	**Column 2**	**Column 3**	**Column 4**
Task Nos. from Attachment A	**Basis of Compensation**	**Invoice Period**	**Compensation**
1	☐ Time & Materials ☒ Fixed Fee	☐ Monthly ☒ Completion of Task(s) ☐ Completion of Work	$ 8,260.00
2	☐ Time & Materials ☒ Fixed Fee	☐ Monthly ☒ Completion of Task(s) ☐ Completion of Work	$ 7,080.00
Part 2 – Reimbursable Expenses			
☐ No expenses are separately reimbursable. The amount(s) in Column 4 of Part 1 include(s) payment for all expenses.		☐ Expenses are separately reimbursable in the maximum amount of:	$
Part 3 – Subconsultant Costs			
☐ Subconsultant costs are ***not*** separately compensable. The amount(s) in Column 4 of Part 1 include(s) subconsultant costs.		☐ Subconsultant costs are separately compensable in the maximum amount of:	$
		Maximum Service Order Compensation (sum of Parts 1 through 3):	$ 15,340.00