PURCHASING SECTION
13450 – 104th Avenue, Surrey, B.C. V3T 1V8
Tel: 604-590-7274 Fax: 604-599-0956
E-mail: purchasing@surrey.ca

ADDENDUM NO. 2

REQUEST FOR PROPOSALS (RFP) NO.:	**1220-030-2018-031**
TITLE:	**INFORMATION TECHNOLOGY PROFESSIONAL SERVICES**
ADDENDUM ISSUE DATE:	**MAY 11, 2018**
CLOSING DATE:	**3:00 P.M. ON MAY 31, 2018 (REVISED)**

INFORMATION FOR PROPONENTS

This Addendum is issued to provide additional information and clarifications to the RFP for the above named project, to the extent referenced and shall become a part thereof. No consideration will be allowed for extras due to the Proponent not being familiar with this addendum. This Addendum No. 2 contains three (3) pages in total.

Q.1. Refer to Section 2.0 DESCRIPTION OF SERVICES on page 13 of the RFP: The Consultants will work on areas of their qualification to assist the City in completing work related its security, architecture and technology practices. Consultants will be required to work as directed in areas including (but not excluding): implementation support, security consulting and advising, troubleshooting, architecture, security risk assessment and penetration testing.

Further, in SCHEDULE C-5 - PROPONENT'S FINANCIAL PROPOSAL, the outline services in section 2.0 DESCRIPTION OF SERVICES is not specified.

For example, security risk assessment and penetration testing in section 2.0 are generally broken out by below categories:

- **Vulnerability Assessment and Penetration Testing**
- **Web Application Security Vulnerability Assessment**
- **Threat and Risk Assessment**
- **Privacy Impact Assessment**
- **Identity Access Management**
- **Privileged Access Management**
- **Incident Response and Remediation Services**
- **Payment Card Industry Compliance ("PCI") Gap Analysis and Report on Compliance**
- **Policy Analysis & Development**
- **Security Strategy and Gap Assessment**
- **Social Engineering Assessment**

Are all above security consulting services required? If so, can we separate by each category above?

A.1. Vulnerability Assessment and Penetration Testing/Web Application Security Vulnerability Assessment and PCI compliance are considered part of Threat and Risk Assessment services. Identity Management is its own category. The City is not currently seeking professional services for:

- **Privacy Impact Assessment**
- **Policy Analysis & Development**
- **Security Strategy and Gap Assessment**
- **Social Engineering Assessment**

Proponents may separate out by each category in their response by simply describing this categorization within the "Typical Support Certification/Training of Staff Assigned" section of the table.

Q.2. Are all below items also considered as part of security assessment?

Application Architecture: Is the Static and Dynamic Code review? Or Web Application Security Vulnerability Assessment?

Network Architecture: Is this categorized as Network Security Architecture? A Network Security Architecture review facilitates a deeper understanding of City's infrastructure and provides a roadmap for improving its security posture moving forward. The assessment will involve the review traffic flows, security design principals, and network & security solutions, as well as perform a series of interviews with key stakeholders, to ensure a complete understanding of your environment's data flows, perimeter security and critical infrastructure. The following network components are reviewed in detail over the course of the assessment:

- **Traffic Flow Review – Gain an understanding of inbound, outbound and inner office traffic flows by reviewing:**
  - Perimeter network design for head office, data centers, remote branches
  - Network security, internal office & inter office segmentation
  - Remote access and connectivity to the customer network

- **Security Design Principals – Understand the organization's security principals and how they are applied to devices on the network through a review of:**
  - Firewall change process
  - Remote access policy
  - Logging and Monitoring requirements
  - SSL inspection policy
  - Authentication management
  - Cloud service usage
  - Endpoint security technology deployment and integration

- **Network & Security Solutions – Identify the locations and capabilities of the various security and network devices including:**

  Security:
  - Firewalls and Next Generation firewalls
  - Intrusion Prevention and Intrusion detection systems
  - Advance Persistence Threat solutions
  - Data Loss Prevention solutions

  Network:
  - WAN acceleration devices
  - Load Balancers
  - Routers
  - Switches

- o Wireless Controllers and APs

A.2. The architecture technical areas are not intended to be "security assessment". The RFP is asking for specific architecture professional services in each of the recognized TOGAF architecture domains. All items identified below are considered part of a Threat and Risk Assessment technical area.

Q.3. Can all below be responded to as above assessment combined?

- **Infrastructure Architecture**
- **Security Architecture**
- **Cloud Architecture**

A.3. No. Anything related to security can be combined under the Security Architecture technical area. However, Infrastructure Architecture and Cloud Architecture are their own architecture domains, and Proponents wishing to be considered for architecture professional services in those architecture domains (or any other architecture domain) must provide a response for that technical area.

END OF ADDENDUM

All Addenda will become part of the RFP Documents.