Coquitlam

Addendum No. 3

City of Coquitlam

RFP No. 21-018

IT - Managed Security Services

Issue Date: May 7, 2021

(consists of 29 pages, including Attachment No. 1 - Revised Proposal Submission Form – Rev No. 1)

Proponents shall note the following amendments to the RFP documents.

R1 – DELETE AND REPLACE

In Proposal Submission Form, Section 7 Corporate Profile, Capabilities and Capacity, the following is deleted:

b) Proponent is to provide an audited copy of their financial statements for the past three (3) years:

Attached to Proposal Submission:

☐ Yes ☐ No

If No, explain:

And replaced with:

b) Proponent is to provide total annual contracts value for similar work for the previous 3 (three) years (2018, 2019, 2020):

Year	Annual Contracts Value	Comments/Additional Information
2020		
2019		
2018		

QUESTIONS AND CLARIFICATIONS

Q1) Since the current environment isn't described, is the City:

a) Currently leveraging an existing security solution that they're looking for a partner to manage for them, or

b) Procuring a Proponent recommended solution they do not possess at this time to purchase, host, and have managed by the Proponent?

A1) Refer to previous Addenda.

Q2) For Device Management, what are the existing security controls in scope (IDS, IPS, FWs, etc...)?
   a) Manufacturer and model(s)
   b) Quantity
   c) Category (e.g. IDS, ISP, FW)

A2) Refer to previous Addenda.

Q3) For Security Operations Center as a Service (SOCaaS), what is in scope for the Proponent to manage?
   a) Manufacturer and model(s)
   b) Quantity
   c) Number of total users for the organization
   d) Required log storage retention period

A3) For questions a, b, and c, refer to Addendum No. 2. For question d, if greater than 1 year is required, then can renegotiate.

Q4) 3.2 Scope of Services – Incident Support "...direct system remediation tasks to onsite responders." Are onsite responders synonymous with City Staff members and/or Contractors?

A4) Yes

Q5) Implementation and Service Methodology - What type of support is the City looking for with respect to the reference towards interfacing with products the City has in place for disaster recovery?

A5) The City is open to hear about full range of Proponents' offerings.

Q6) Security Event Monitoring - The assumption in this requirement is that the City currently has a firewall, IDS, and IPS solution implemented. Is the nature of this requirement to monitor these assets directly or via the partner recommended SIEM solution whereby logs from these assets are ingested and monitored for events, analysis, and response?

A6) Yes

Q7) Security Information Management - in reference to the City's raw event logs, we require clarity as follows:
   a) Log sources by Quantity and Type
   b) Manufacturer and Model for each source
   c) Number of total users for the organization within this scope

For standard data retention policies, our standard is 1 year. Any requirement beyond 1 year would be scoped and priced accordingly. The City needs to confirm desired retention time period.

A7) If greater than 1 year is required, then can renegotiate.

Q8) Advanced Analytics and Capabilities - with respect to network monitoring and/or network forensic features, capabilities, offerings, is the City looking to purchase these solution types?

A8) Refer to previous Addenda.

Q9) With the City being a O365 client/user can you share with us what Microsoft Licenses do you currently have? i.e. E3 or E5?

A9) E3

Q10) What is the City's current PCI level?

A10) Level 3

Q11) Has the City of Coquitlam completed a risk assessment?

A11) No

Q12) How many external facing IPs are in scope for PCI vulnerability scanning?

A12) Refer to previous Addenda.

Q13) Is there an expectation that we use your existing Tenable license for vulnerability scans?

A13) Open to recommendation

Q14) You mention Penetration Testing. Are you looking for both an internal and external Penetration Test?

A14) Both

Q15) What database vendor have you standardized on (useful to know for scoping a database Pen test)?

A15) Oracle

Q16) Are there any web applications that require vulnerability scanning and penetration testing?

A16) Yes

Q17) Are any web applications in-scope for PCI?

A17) Yes

ATTACHMENT No. 1

REVISED PROPOSAL SUBMISSION FORM
REV NO. 1

City of Coquitlam

REQUEST FOR PROPOSALS

RFP No. 21-018

IT Managed Security Services

Proposals will be received on or before 2:00 pm local time on

~~**Friday May 14, 2021**~~

Friday May 21, 2021

(**Revised - Closing Date and Time)**

INSTRUCTIONS FOR PROPOSAL SUBMISSION

Proposal submissions are to be consolidated into one PDF file and uploaded through QFile, the City's file transfer service accessed at website: qfile.coquitlam.ca/bid

1. **In the "Subject Field" enter:** RFP Number and Name
2. **Add files in .pdf format and "Send"**
   (Ensure your web browser remains open until you receive 2 emails from Qfile to confirm upload is complete.)

Proponents are responsible to allow ample time to complete the Proposal Submission process. If assistance is required phone 604-927-3037.

REVISED PROPOSAL SUBMISSION FORM – Rev No. 1

Complete and return this Proposal Submission Form - along with:

☐ **Sample Invoice attached**
☐ **Proposed SLA's attached**

Submitted by: _____
(company name)

Proponents are to provide as much information as possible when replying to each point throughout the Proposal.

Proponents MUST identify any specific requirements with which they are unwilling or unable to comply.

1. PRICE

The pricing provided shall be all inclusive without limitation, including all labour, wages, benefits, equipment, overhead and profit. All Pricing is to be held firm for the length of the Term.

1.1. Scope of Services

Proponents are to provide pricing for a three (3) year and a five (5) year Term for the Services as described in the Scope of Services:

SERVICES		3 Year Term	5 Year Term
a) Start-up & Implementation Services	**Unit of Measure (State)**	**Price**	**Price**
One-time , all inclusive onboarding:		$	
Other (please list below, if any including details on the number of devices or data sources (e.g., IDS sensors, firewalls and servers))			
		$	
		$	
TOTAL - START-UP & IMPLEMENTATION SERVICES			

SERVICES		3 Year Term	5 Year Term
b) Recurring Annual Charges – Pricing and details on one-time and recurring charges.	**Unit of Measure (State)**	**Price**	**Price**
List and describe any recurring annual charges using the spaces below including details on the number of devices or data sources (e.g., IDS sensors, firewalls and servers) and storage cost depending on retention policy (1 yr, 3 yrs, 7 yrs):			
		$	
		$	
TOTAL - RECURRING ANNUAL CHARGES			

SERVICES		3 Year Term	5 Year Term
c) Other Charges/Fees	**Unit of Measure (State)**	**Price**	**Price**
List and describe any other charges using the spaces below:			
		$	
		$	
TOTAL - OTHER CHARGES/FEES			

1.2. Software and Third Party Products

Provide pricing and any licensing and warranty information for third-party products you may require the City of Coquitlam to purchase in support of this service.

Software/Product	Unit of Measure	Price	Licensing/Warranty Information

1.3. Optional - Additional Services

Proponents are to provide firm pricing for a three (3) year and a five (5) year Term for the Optional – Additional Services proposed:

SERVICES		3 Year Term	5 Year Term
Additional Services (include description and functionality) e.g incident response activities, including breach response services, etc.	**Unit of Measure (State)**	**Price**	**Price**
		$	$
		$	$
		$	$
		$	$

1.4. Hourly Rates

The following are hourly and daily rates for qualified personnel that would be used for valuing additional hours on an "as needed and when requested" during the MSSP engagement.

Role/Position/Task	Hourly Rate	Daily Rate

1.5. Pricing – Other

a) How is Pricing negotiated for upgrading or expanding services? Can the City add devices or data sources without affecting Pricing or Services?

b) How would the purchase of new security devices (or upgrade of the City's current devices) affect Pricing?

2. REQUESTED DEPARTURES – CONTRACT

The Proponent has reviewed the City's Contract and the Standard Terms and Conditions - Consulting and Professional Services

I/We would be prepared to enter into that Contract, amended by the following departures (list, if any):

3. VALUE ADDED

Provide information on what makes your firm innovative, what is your competitive advantage, and what other services your firm provides that would assist or be of benefit to the City:

4. SUSTAINABLE BENEFITS AND SOCIAL RESPONSIBILITY

4.1. Sustainable Benefits

Describe all initiatives, policies, programs and product choices that illustrate your firm's efforts towards sustainable practises and environment responsibility in providing the services that would benefit the City:

4.2. Social Responsibility

a) What policies does your organization have for hiring apprentices, indigenous peoples, recent immigrants, veterans, young people, women, and people with disabilities:

b) What policies does your organization have for the procurement of goods and services from local small and medium sized business or social enterprises:

5. CONFLICT OF INTEREST DECLARATION

Proponents shall disclose any actual or potential conflicts of interest and existing business relationships it may have with the Cities, their elected or appointed officials or employees:

6. AGREEMENTS AND LICENSING

a) Indicate and describe the licensing model(s) for your MSSP offering.

b) Provide any licensing and warranty information for third-party products you may require the City to purchase in support of this service.

c) What is the Proponents contract liability limitation if the Services that are performed failed (i.e. security breach).

7. CORPORATE PROFILE, CAPABILITIES AND CAPACITY

a) Proponent to provide the name, title and appropriate contact information of the authorized negotiator and signatory.

Authorized Negotiator	Authorized Signatory
Name:	Name:
Title:	Title:
Phone:	Phone:
Email:	Email:

b) Proponent is to provide total annual contracts value for similar work for the previous 3 (three) years (2018, 2019, 2020):

Year	Annual Contracts Value	Comments
2020		
2019		
2018		

c) Proponent is to state how many years they have been in business and organizational history (e.g. mission, vision, corporate directions, etc.)

d) Proponent is state the location of the company headquarters and list and provide locations for each security operation centre it manages:

e) Proponent is to state how many years that they have been in business providing MSSP?

f) Proponent is to provide a sample monthly invoice that clearly represents the type of information the Proponent would provide in support of charges itemized on the invoice for the Services contemplated in their Proposal:

Attached to Proposal Submission:

☐ Yes ☐ No

If No, explain:

g) Proponent is to state the number of years that they have offered each of the Services in the MSSP and provide the number of clients and annual revenue for each service:

Services	Number of Clients	Annual Revenue

h) Proponent is to state any alliances with other companies you have that are related to your MSSPs, such as using a third-party software as part of your MSSP portfolio.

i) Proponent is to provide a narrative as to their experience and capabilities in delivering goods and Services similar to those requested in this RFP:

j) Proponent is to provide a narrative as to their capacity to take on this service Contract with respect to manpower and other contracts that may affect their ability in delivering the goods and Services within the timeline expectations of the City:

8. QUALIFICATIONS AND STAFFING

a) Proponent is to state how many customers they have using MSSP:

b) Proponent is to state the total number of employees in your company and the number of employees responsible for MSSP delivery:

c) Proponent is to provide the relative distributions of employees in your MSSP company providing delivery, project management, customer service, and how these employees are geographically distributed:

Description	Amount	Location
Project Management Team Members		
Customer Service Team Members		
Support Desk Team Members		
Level 2 desk team members		
Level 3 team members		

d) Proponent is to list percentage of your staff possessing security certifications (list the certifications), and what is the average number of years of experience they have in performing security monitoring or security consulting?

Certification	Percentage	Years Experience

e) Provide the Proponent's job description and resume for the security-monitoring personnel. Include a summary of the technical expertise and/or special capabilities required. (Attach resume and job description to Proposal Submission)

Name of Personnel	Technical Expertise and Special Capabilities	Resume Attached

f) Proponent to describe their process for screening and hiring their MSSP staff including required certifications local law enforcement clearance:

g) Proponent to explain the process of initial and ongoing training of your security-monitoring staff.

h) Proponent to state ratio of monitored security devices to personnel and ratio of managed security devices to personnel?

Function	State Ratio
Monitored security devices to personnel	
Managed Security devices to Personnel	

i) Proponent is to state the average length of employment of an MSSP analyst with your company?

j) Proponent is to describe MSSP customer support tiers.

k) Proponent is to state any industry certifications/attestations the Proponent's SOC(s) hold, such as Statement on Standards for Attestation Engagements (SSAE) 16 Type 2, or International Organization for Standardization (ISO) 27001. (Attach evidence/supporting documentation to Proposal Submission)

Certifications/Attestations	Evidence / Supporting Documentation Provided

9. EXPERIENCE AND REFERENCES

Proponents shall be competent and capable of performing the services requested and successfully delivered service contracts of similar size, scope and complexity.

Description of Contract	
Year Started	
Year Completed	
Company	
Contact Person	
Telephone and Email	
Contract Value	

Description of Contract	
Year Started	
Year Completed	
Company	
Contact Person	
Telephone and Email	
Contract Value	

Description of Contract	
Year Started	
Year Completed	
Company	
Contact Person	
Telephone and Email	
Contract Value	

10. SUB-CONTRACTOR

The following Sub-contractors will be utilized in provision of the Services and will comply with all the terms and conditions of this RFP:

Type of Service	Company Name	Phone	Years of Experience and Qualifications

11. IMPLEMENTATION AND SERVICE METHODOLOGY

a) Proponent to provide a brief overview of the managed security services and any supporting products:

b) Does Proponent staff their SOC(s) 24/365? Provide details.

c) Proponent to describe their approach to supporting 24/365 remote security event monitoring and device/agent management, including any use of "follow the sun" staffing.

d) Proponent to describe the architecture of their MSSP delivery capability, including elements in your SOC, data center (on your premise, colocations, and private and public cloud services), network and our premises, as well as the centrally delivered log management, analytics and portal tiers, and capabilities for collecting event logs and data from other locations (e.g., software as a service [SaaS] and infrastructure as a service [IaaS]). Provide example architectural diagrams and descriptions. Finally, include and identify any elements that are delivered by third-party partners.

e) Proponent to list the primary tools used to deliver the Services.

f) Proponent is to explain how the Services, and any supporting products will use or interface with products the City has in place for disaster recovery. Include details on how you intend to connect to City's infrastructure to provide support:

g) Proponent is to state if the Services require the use of proprietary technology that the City must purchase or install? If so, please list all pertinent information related to this technology, including hardware, software, networking, middleware and database requirements.

h) Proponent is to explain how external data is used (e.g., threat intelligence feeds) to analyze potential threats to the City's environment, and describe what access to this data will be provided to the City.

i) Proponent is to provide an overview of your customer notification and escalation process. Include details on how often a customer is notified of a security event, and on the methods of notification.

j) Proponent is to state how the Services will be delivered to the City if on premise, cloud or hybrid.

k) Proponent is to explain how they will complete an initial assessment, and the method of establishing a baseline security level. Include specifics on your implementation timeline; infrastructure requirements; data transfer, data storage and segregation, and backup systems; and encryption standards.

l) Proponent is to describe the frequency and opportunities for continuous improvement during the implementation phase.

m) Proponent is to provide an example of how the Proponent's services detected and addressed a recent security incident.

n) Proponent is to provide their methodology for detecting custom or targeted attacks directed at our users or systems.

12. SECURITY EVENT MONITORING

a) Proponent to describe the capabilities of the Services to monitor the City's firewall, intrusion detection system (IDS), intrusion prevention system (IPS) and vulnerability data.

b) Proponent is to describe their use of signature-based and correlation rules.

c) Proponent is to provide a narrative to their ability to analyze this data and to provide real-time event correlation between data sources, and real-time alerting of security incidents and system health incidents.

d) Proponent is to describe how their company keeps signatures/rules updated.

e) Proponent is to describe their support for the creation and management of customized correlation rules. Explain the capabilities available to City staff for doing so. Describe any limitations, such as data sources, age and query frequency.

f) Proponent is to describe their ability to analyze collected data to identify when changes in behaviors of users or systems represents risk to the City's environment.

g) Proponent is to state their methodology for reducing false positives and false negatives and for classifying security-related events that represent a risk to the City.

h) Proponent is to describe how false positives are managed, and how the Proponent will incorporate false positive feedback from the City.

i) Proponent is to describe the typical workflow and process that occurs when the security analytics detects a security event, beginning with how that is presented to a SOC analyst for evaluation through the triage, validation, prioritization and customer alerting/notification process. Indicate where activities are automated versus manually performed by analysts.

j) Proponent is to state the level of interaction and support that City staff can expect from your security analysts to assess, investigate and respond to incidents.

13. SECURITY DEVICE MANAGEMENT

a) Proponent is to explain their process for updating software to include signature updates and system patches. How do you ensure that this is done in a nonintrusive manner to your customers?

b) For each management service, the Proponent is to describe the change management process and the Proponent's willingness to modify the process to meet the City's requirements.

c) For device management services, The Proponent is to indicate whether changes are reviewed to assess increased risk, exposure or the effects on capacity.

14. SECURITY INFORMATION MANAGEMENT

a) Proponent is to provide the data sources supported for log collection, reporting and retention. Can logs be collected from any source? Describe the collection methods (e.g., forwarded syslog, Windows Management Instrumentation [WMI], local forwarding agent).

b) Will the Proponent collect all of the City's raw event logs and data and forward to your platform for storage? If no, describe the variation and options for full log event retention (if applicable).

c) Will the City's logs be compressed and encrypted in transit, and is it a guaranteed delivery via a store and forward type of solution? Please describe.

d) Proponent is to indicate any limitations to your log collection capabilities, such as peak event rates, volume or sources.

e) Proponent is to explain the capabilities that allow City staff to search and browse original log data. Describe any limitations to this capability.

f) Proponent is to describe the capabilities of City staff to create and modify reports based on collected log data. Indicate any limitations, such as number of reports, complexity of queries and age of data.

g) Proponent is to state their standard data retention policies and ability to modify them to meet the City's requirements.

h) Proponent is to state minimum and maximum length of time that log retention can be offered? Describe what is actively available versus what is kept offline.

i) Proponent is to state the process for adding additional log sources to the Services? Include the implications for deployment architecture, integration costs and ongoing costs.

15. ADVANCED ANALYTICS AND CAPABILITIES

a) Proponent is to describe the ability to implement watch-lists, both those the Proponent defines, and those the City defines.

b) What technologies does the Proponent use to enable advanced analytics?

c) Proponent is to describe any specific network monitoring and/or network forensics features, capabilities or offerings to detect advanced, targeted attacks.

d) Proponent is to describe any specific endpoint behavior analysis and/or endpoint forensics features, capabilities or offerings to detect advanced, targeted attacks.

e) Proponent is to describe the data and threat visualization capabilities available to the City via the portal.

f) Proponent is to describe any managed detection and response-type service offerings (e.g., managed endpoint detection and response, threat hunting, remote response and containment).

16. VULNERABILITY MANAGEMENT SERVICES

a) Proponent to describe their service capabilities to monitor vulnerability scans internally and externally with the organization.

b) Proponent is to indicate the technologies used to conduct scans, both commercial and open source.

c) Proponent is to provide details on the methodology for collecting and analyzing vulnerability and asset data (e.g., configuration) from all sources in scope.

d) Proponent is to describe the process by which vulnerabilities are triaged and prioritized prior to reporting, including the integration of previous scan results and actions carried out.

e) Proponent is to state if vulnerability scans be scheduled, initiated/managed via your MSSP portal? How are results viewed in the portal? Indicate your ability to intake results from scanning devices already situated in the City.

f) How frequently is the vulnerability database updated, and what are the data sources used for that?

g) Proponent is to state the application-specific scanning used as part of their VM services.

17. INCIDENT RESPONSE

a) Are there any remote and/or on-site incident response (IR) activities included as part of the Services? If so, describe the services provided, including specifics on what is included in the Scope of Services versus what is available as Optional – Additional Services.

b) Does the Proponent provide incident response activities, including breach response services, via an optional retainer? If so, describe the packages, service-level agreements (SLAs), and included services. Does the Proponent offer proactive services as part of a retainer? Which services are able to be delivered remotely (both proactive and reactive), and which require your staff to be physically on our site(s)?

c) Does the Proponent provide any IR activities outside of a retainer, such as a "just in time" type services?

d) If the Proponent provide IR services, please describe the methodology for escalation and triage of incidents. What are the Proponent's investigative capabilities?

e) Does the Proponent assist with creating specific IR use cases and maintaining a run book? If so, describe how this is achieved.

f) Describe any self-service features for incident response provided via the portal (e.g., automated malware analysis, custom signature or correlation rule implementation).

18. PORTALS, REPORTS AND DASHBOARDS

a) Proponent to describe the information provided by and features available through the web-based portal or console associated with the Services. Include details on Proponent's support for RBAC, customization of screens and data presentation, predefined correlation rules, and predefined reports.

b) Proponent to state whether all Services and MSSP features, including those delivered by partners, will be available via a single portal, regardless of region or part of business delivering the Services.

c) Proponent to state authentication and identity management system used by their portal?

d) How does the portal provide the City access to external threat intelligence feeds, in addition to the City's own threat intelligence feeds?

e) Can the City access and search log event data via the Proponent's MSSP portal?

f) Proponent is to state user roles available to the City for the MSSP portal (e.g., administration, view/report, etc.). Describe how user access to data and reports can be restricted based on role and group.

g) Proponent is to describe any real-time chat/instant messaging and/or live video interaction available for City staff to communicate with the Proponent's SOC staff.

h) Describe any integration capabilities with third-party service desk and ticketing tools and services. How is this achieved (e.g., email, application programming interfaces [APIs], etc.)? Also, Proponent is to indicate if you single-direction or bidirectional support is provided, and whether the integrations are subject to additional costs.

i) Describe the portal capabilities to enable City staff to create, update and close tickets.

j) Describe how much visibility the Proponent provides on the tasks of the workflow. Consider how many alerts there are, your staff level (e.g., Level 1, Level 2, Level 3), and how long they are on a particular phase in the process.

k) Is there a smartphone/tablet application available? If so, briefly describe the supported platforms and functionality.

l) Describe operational, regulatory and executive reporting capabilities.

m) Indicate the number of predefined reports, including specific regulatory and compliance (e.g. HIPPA, PCI DSS) items supported, that will be available to the City. Please provide examples.

n) Explain how report data can be exported to or used by an external report writer or risk dashboard.

o) Explain the capabilities for City staff to create customized, ad hoc queries and reports. Describe any limitations to ad hoc query or report generation, including data sources, data age and query frequency.

19. SERVICE MANAGEMENT

a) Explain the expected working relationship, roles and responsibilities between your security staff and City's Technical Services staff.

b) Indicate the frequency of meetings or teleconferences to review performance, issues, threat environment and responses. Explain the types of analyst and account management support provided during those meetings.

c) Indicate device/agent management, and real-time event management notification service levels. Explain how they are measured, and how they will be communicated to the City.

d) Provide a sample of an SLA as outlined in the Services, in addition to the service onboarding and delivery phases.

Sample SLA Attached ☐ YES ☐ NO

If No, state why:

e) Proponent to describe their problem resolution and escalation procedure.

f) Proponent to describe their SLA performance reporting. If applicable, indicate whether these methods are used in some or all regions.

g) Does the Proponent have standard time frames, after which a given security product is no longer supported? If so, please describe the details, including proprietary and third party software time frames.

h) Please provide details on support agreements. If a third party software update is required, when does the SLA between the Proponent and the City begin?

i) Describe the process for adding services or new technologies. For example, assume that the City adopted a deep-packet-inspection firewall technology —how would this be supported and incorporated into an SLA?

j) How will the Proponent ensure that all licensing, SLA's etc. will Co-Terminate upon the Contract End Date?

k) What process will determine if a change is within the original scope of the supplied technology or a new feature? How will the costs be determined?

l) What access to internal-auditing documentation will you provide if our auditors, customers or business partners require this documentation in support of legal, regulatory or contractual requirements? What is your process for requesting documentation? What are the time frames to which you will commit for producing documentation?

m) Proponent to provide resolution process for complaints the City may have.

n) Proponent to state their process for notifying the City of the City's noncompliance with the SLA, and for notifying the Proponent of the Proponent's non compliance with the SLA.

o) Describe the remedies available to the City should the Proponent fail to meet any SLAs.

p) Outline early termination penalties and charges. Describe how the costs are calculated to extract all captured data to be moved to another MSSP, if applicable?

q) Describe how the City's data would be returned to the City during the termination process.

r) Describe how the City's data (including data generated by your company about security events and incidents affecting the City) will be governed and protected in transit. Consider this from a technology perspective, as well as via processes and procedures. How will the treatment of the City's confidential data assist with better job performance (e.g., creating internal architecture and topology maps)?

s) Provide examples of how the Proponent has met specific regulatory or statutory requirements to the data within Canada and specifically British Columbia.

20. ADDENDA

We acknowledge receipt of the following Addenda related to this Request for Proposals and have incorporated the information received in preparing this Proposal:

Addendum No.	Date

21. AUTHORIZATION

We hereby submit our Proposal for the supply and services as specified and undertake to carry out the work in accordance with all Regulations and Codes, applicable to this RFP.

We agree to the rules of participation outlined in the Instructions to Proponents and should our Proposal be selected, will accept the City's Contract Standard Terms and Conditions - Consulting and Professional Services.

The signature is an authorized person of the organization and declares the statements made in their submission are true and accurate.

For the purpose of this RFP submission, electronic signatures will be accepted.

Company Name:	
Address:	
Phone:	
GST Registration No.:	
Project Contact: Name and Title of Individual *for communication related to this RFP* (please print)	
Contact Email:	
Name & Title of Authorized Signatory: (please print)	
Signature:	
Date:	

End of Addendum No. 3

Proponents take into account the content of this Addendum in the preparation and submission of the Proposal which will form part of the Contract and should be acknowledged on the Proposal Submission Form.

Upon submitting a Proposal, Proponents are deemed to have received all addenda that are issued and posted on the City's website and considered the information for inclusion in the Proposal submission.

Issued by:

M. Pain, Purchasing Manager
bid@coquitlam.ca