Coquitlam

City of Coquitlam

Request for Proposals
RFP No. 21-018

IT – Managed Security Services

Issue Date: April 23, 2021

TABLE OF CONTENTS

SUMMARY OF KEY INFORMATION

RFP Reference	**RFP No. 21-018** **IT Managed Security Services**
Overview of the Opportunity	The purpose of this RFP is to invite Proposals from qualified firms for the provision of **IT Managed Security Services.**
Closing Date and Time	**2:00 pm local time** **Friday May 14, 2021**
Instructions for Proposal Submission	Proposals are to be consolidated into one PDF file and uploaded electronically through Qfile, the City's file transfer service accessed at 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 receipt.) Phone 604-927-3037 should assistance be required. The City also reserves the right to accept Proposals received after the Closing Date and Time.
Obtaining RFP Documents	RFP Documents are available for download from the City of Coquitlam's website: http://www.coquitlam.ca/Bid-Opportunities Printing of RFP documents is the sole responsibility of the Proponents.
Instructions to Proponents	The guidelines for participation that will apply to this RFP are posted on the City's website: Instructions to Proponents
Questions	Questions are to be submitted in writing quoting the RFP number and name up to 3 business days before the Closing Date sent to email: bid@coquitlam.ca
Addenda	Proponents are required to check the City's website for any updated information and addenda issued, before the Closing Date at the following website: www.coquitlam.ca/Bid-Opportunities
Withdrawal of Submission	Proposals may be withdrawn by written notice only, made by an authorized representative of the Proponent sent to email: bid@coquitlam.ca prior to the Closing Date and Time.
Terms and Conditions of Contract	City of Coquitlam Standard Terms and Conditions - Consulting and Professional Services are posted on the City's website and will apply to the Contract awarded as a result of this RFP.

DEFINITIONS

"Agreement" "Contract" means the contract for services or City Purchase Order that will be issued to formalize with the successful Proponent through negotiation process with the City based on the Proposal submitted and will incorporate by reference the Request for Proposals, Specifications, Drawings, any additional subsequent information, any addenda issued, the Proponent's response and acceptance by the City.

"City" "Owner" means City of Coquitlam;

"Consultant" "Contractor" means the person(s) firm(s) or corporation(s) appointed by the City to carry out all duties, obligations, work and services described in the Request for Proposal and all associated documentation, which may also include mutually agreed revisions subsequent to submission of a Proposal. "Consultant" "Contractor" and "Proponent" are complementary in terms of duties, obligations and responsibilities contemplated at the Request for Proposals stage, through evaluation process, execution and performance of the services and works.

"MSSP" means Managed Security Services Portfolio

"Price" means the amount that will be paid by the City to the Contractor for delivery and acceptance of goods and Services;

"Proponent" means responder to this Request for Proposals;

"Proposal" means the submission by the Proponent;

"RBAC" means role-based access control

"Request for Proposals" "RFP" shall mean and include the complete set of documents, specifications and addenda incorporated herein, and included in this Request for Proposals;

"Services" "Work" "Works" means and includes the provision by the successful Proponent of all services, duties, and expectations as further described in this RFP. This will also mean the whole of the work, tools, materials, labour, equipment, travel, and all that is required to be done, furnished and performed by the Contractor;

"Shall" "Must" "Will" "Mandatory" means a requirement that must be met;

"SOC" means Security Operations Centre;

"Supply" "Provide" shall mean supply and pay for and provide and pay for.

1. INSTRUCTIONS TO PROPONENTS

1.1. Purpose

The City Invites Proposals from qualified, experienced companies to provide labour, equipment, materials, overhead and all that is necessary for the provision of Managed Security Services for the City's ICT department.

1.2. Instructions to Proponents

Proponents are advised that the rules for participation that will apply to this RFP are posted on the City's website at: Instructions to Proponents.

By submission of a proposal in response to this RFP, the Proponent agrees and accepts the rules by which the RFP process will be conducted.

Proponents should complete and submit the information requested in this RFP document on the Proposal Submission Form.

1.3. Term of Contract

The City will consider a three (3) year or a five (5) year Term for the Contract, based on what provides best value to the City.

1.4. Proposal Submission

Proponents should complete and submit the information requested in this RFP document on the Proposal Submission Form or in a format that has been approved and is acceptable to the City.

1.5. Requested Departures

The Proponent acknowledges that the departures requested in the Proposal Submission Form will not form part of the Contract unless and until the City specifically consents in writing to any of them. The City will evaluate those departures as per the Evaluation Criteria stated within this RFP.

1.6. Evaluation Criteria

The criteria for evaluation of the Proposals may include, but is not limited to:

Corporate Experience, Capacity and Resources – 30 points

- Corporate Profile, Capabilities and Capacity
- Qualifications and Staffing
- Experience and References
- Sub-contractors
- Requested Departures

Technical – 40 points

- Implementation and Service Methodology
- Security Event Monitoring
- Security Device Management
- Security Information Management
- Advanced Analytics and Capabilities
- Vulnerability Management Services

- Incident Response
- Portals, Reports and Dashboards
- Service Management

Financial and Value Added – 30 points

- Pricing,
- Hourly Rates
- Consulting Hours provided
- Termination costs
- Co-Termination
- Value Added
- Sustainability and Social Responsibility

These criteria will be used to determine best overall value to the City. Proposals will be compared to select one or more that are most advantageous.

And, upon selection of one or more lead Proponent(s):

- References may be contacted
- Interviews may be conducted

The City reserves the right to check references even if they are not specifically listed. Information obtained from references will be confidential and will not be disclosed to any Proponents.

The City may, at its discretion, request clarification or additional information from a Proponent with respect to any Proposal and the City may make such requests to only selected Proponents. The City may consider such clarifications or additional information in evaluating a Proposal. Proponents may be required to sign the City's Non-Disclosure Agreement prior to a clarification or a request for additional information.

Proponents agree the City may disclose names of Proponents and total award amount, however, unevaluated results, unit prices, rates or scores will not be provided to any Proponents. Incomplete Proposals or Proposals submitted on forms other than the Proposal Submission Form may be rejected.

The City has no obligation to accept any Proposal if that Proposal is the sole bid. The lowest price of any Proposal will not necessarily be accepted but will be analyzed to determine best overall value.

The City reserves the right to reject without further consideration any Proposal which in its opinion does not meet the criteria it considers essential for the work outlined in this RFP.

1.7. Eligibility

For eligibility, and as a condition of award, the successful Proponent would be required to meet or provide the equivalent:

a) Commercial General Liability (CGL) insurance $5M coverage provided and Professional Errors and Omission's Liability insurance $1M coverage provided on the City's Certificate of Insurance - Consultant Form

b) Be registered and provide WorkSafeBC clearance

c) Accept the City's standard Terms and Conditions posted on the City's website: Standard Terms and Conditions - Consulting and Professional Services, including any privacy related provisions the City may include in the Contract

d) A City of Coquitlam or Tri Cities Intermunicipal Business License

e) Complete the City's standard Privacy Impact Assessment

f) Complete and submit the City's Non-Disclosure Agreement.

These items are not required as part of this Proposal Submission but will be required prior to entering into an agreement with the City for Services.

1.8. Prices

Prices shall be all-inclusive and stated in (Canadian Funds). Prices shall remain FIRM for the Initial Term of the Contract.

Prices shall include the provision of all tools, materials, equipment, labour, transportation, fuel, supervision, management, overhead, materials, services, all other associated or related charges, foreign, federal, and provincial taxes, and all other requirements necessary for the commencement, performance and completion of Services as described.

Taxes are to be shown separately at time of invoicing.

1.9. Examination of Proposal Documents

The Proponent must carefully examine the Proposal Documents. The Proponent may not claim, after the submission of a Proposal, that there was any misunderstanding with respect to the requirements and conditions imposed by the City.

There will be no opportunity to make any additional claim for compensation or invoice for additional charges that were not considered and included in the Proposal price submitted, unless the City, at its sole discretion, deems that it would be unreasonable to do so, or there are additional work requirements due to unforeseen circumstances.

All information in this RFP Document, Drawings, Specifications, and any resulting Addenda will be incorporated into any Contract between the City and the successful Proponent, and therefore must be considered by the Proponent in preparing their Proposal.

2. GENERAL CONDITIONS OF CONTRACT

2.1. Terms and Conditions

The City's Standard Terms and Conditions - Consulting and Professional Services, as published on the City's website, the Conditions listed below, along with the accepted Proposal, addenda and any subsequent clarifications, correspondence, the totality of which will constitute the Contract.

In addition, the following terms and conditions will also apply to this Contract:

2.2. Operations and Coordination of the Services

The Contractor shall agree to coordinate the execution of the Services with the City such that disruption of the work of all involved is minimized.

2.3. Regulatory and Compliance Requirements

Contractor is to comply with the latest regulatory and compliance requirements, including all provincial and other amendments, and local by-laws. When multiple codes and/or regulations apply, follow the most stringent provision:

- Payment Card Industry Data Security Standard (PCI DSS)
- BC's Personal Information Protection Act, SBC 2003 c. 36
- Federal Personal Information Protection and Electronic Documents Act, SC 2000 c 5
- Freedom of Information and Protection of Privacy Act, RSBC 1996, c 165 (FIPPA)
- SOC 2 compliance

3. SCOPE OF SERVICES

3.1. General Requirements

The City requires a qualified, experienced company to provide support services to setup, manage, operate and maintain a Security Operations Centre (SOC) to enable the City to prevent, detect, respond and recover from cyber security threats and events. The core services to be acquired under this RFP will include 24 hours per day, 7 days per week, 365 days per year (24x7x365) threat intelligence and reporting, network monitoring and security event triage, analysis, and alerting, and computer security incident response/support.

The City may elect to award some, all or none of the Optional - Additional Services that the Proponent offers to the City.

3.2. Scope of Services

The Services to include but not limited to:

a) Security Operations, Monitoring and Reporting of City's System(s):

- System security events on a 24/7x365 basis
- Provide notification, escalation, and daily summary reports based on gathered threat intelligence and security event analysis, ensuring that these threats are actionable
- Monitor and analyze security event data to include investigation of reported incidents using system logs and other means of detection
- Provide event analysis and evaluation of the reported incident and provide categorization, prioritization, and recommendation of containment measures
- Document all event investigation activities, incoming requests for information, or suspected incident reports as required to support the City's incident management process
- Review audit logs and record any inappropriate and/or illegal activity in order to reconstruct events during a security incident. This includes monitoring network and host devices and reporting incidents to the City Security Staff.
- Provide written reports detailing all security events and submit these reports, according to established procedures and reporting requirements.
- Investigate and positively identify anomalous events detected by security devices or reported to the City from external entities, system administrators, and the user constituency
- Ensure all SOC systems and applications are available and operational

b) Incident Support

- Perform remote incident handling support such as forensics collections, intrusion correlation tracking, threat analysis and direct system remediation tasks to onsite responders
- Provide remedial recommendations and produce comprehensive report on findings

c) Threat analysis and intelligence

- Detect, monitor, analyze, and mitigate targeted, highly organized, or sophisticated threats
- Maintain situational awareness of current activity and risks to the City

- Leverage all sources of intelligence to develop information on cyber threats and to perform advanced technical analysis on incidents that occur on the City's networks
- Perform consolidated and comprehensive information and intelligence analysis of threat data obtained from various sources to provide indication and warnings of impending attacks against the City's networks
- Provide reporting on technical network and host based attack vectors, emerging cyber threats, new vulnerabilities, and current trends used by malicious actors
- Create and maintain databases to catalog and track ongoing threats to the City's networks

d) Documentation and Standard Operating Procedures

- Create diagrams of new or revised security deployments before they are transitioned to operational support. This documentation must encompass all systems and applications which comprise and support the SOC.
- Develop SOC standard operating procedures (SOP) and revise them when changes to SOC operations occur.
- Provide daily, weekly, and monthly written reports consisting of a summary of all SOC activities, performance metrics, security incident status and actions accomplished for the period.
- Submit the following reports to the City
  - Monthly status reports on the progress made during the current period
  - planned activities and problem/issues with recommended solutions,
  - anticipated delays, and resources expended

e) Advance Incident Management Support, Forensics and Malware Analysis

- Conduct on-site or remote coordinated computer security incident management, response, and recovery support, as required
- Perform advanced technical analyses of potentially malicious activities that have occurred or are believed to have occurred on the City's network via security event data from the SOC
- Perform endpoint/host-based forensics and memory analysis
- Perform triage and in-depth malware and reverse malware analysis of malicious Windows software and phishing emails, and other client-side exploits, to support the resolution of security incidents
- Perform digital forensics on media associated with compromised hosts to assess the scope and nature of intrusions
- Reverse engineer the sequence of events of a breach or attack
- Perform static and dynamic file analysis to identify malware characteristics, intent and origin
- Recommend countermeasures to malware and other malicious code and applications that exploit the City's hosts, endpoints, network and data communication systems
- Develop recommended changes to policies and procedures that will strengthen the investigative capabilities of malware incidents for the City's network infrastructure
- Advanced traffic analysis (at the packet level) and reconstruction of network traffic to discover anomalies, trends, and patterns affecting the City's networks

f) Ongoing Vulnerability Assessments and Security Assurance Scans

- Perform regularly scheduled (monthly and ad hoc) Vulnerability Assessments (VA's) using a master schedule agreed to
- Coordinate the VA testing in advance with the City to ensure minimal disruption with planned network maintenance, availability, and operations
- Use approved test procedures, scripts, and VA tools including the latest versions of tools with up to-date lists of vulnerability checks, appropriate to the City's policies, needs and technologies
- Conduct specialized VA testing to include Database and Web application assessments, penetration testing, and Wireless technology testing and analysis as part of planned security assurance activities or change requests for new or changed systems and architecture
- Prepare and submit security testing Rules of Engagement (ROE) for approval prior to conducting of penetration testing
- Employ ad-hoc or emergency VA scanning to support targeted incident investigation, escalation and emergency response to security events in accordance with documented procedures
- Develop reports, findings, and recommendations to mitigate security gaps and vulnerabilities and provide support to Cyber Security by interpreting scan results and recommend remediation plans
- Provide VA summary reports of the testing and document the findings

g) Maintain and operate security technology

- Maintain the Security Information and Event Manager (SIEM) to collect data from network sensors, raw data from collection agents, firewalls, web proxy and content filtering, DLP, antivirus, and vulnerability scanner elements
- Conduct administration, management, and configuration of the SOC tools (e.g., SIEM, IDS, and DLP, devices and application systems, dedicated servers and sensors)
- Develop security device signatures, performance reports, and metrics
- Tune the SIEM and IDS/Intrusion Prevention System (IPS) events to minimize false positives
- Continuously operate, manage, update and configure all security technology including the Security Information and Event Management (SIEM) System, IDS/IPS, and other potential security technology forming part of the SOC and security operations
- Ensure logging of appropriate security feeds and correlation to the SOC SIEM tool
- Install or modify network security components, tools, and other systems as required to maintain optimal coverage and performance

3.3. Optional - Additional Services

Proponents are encouraged to provide detail to additional services that are available outside of 3.2 Scope of Services. (i.e.: services available that specifically identify advanced, targeted, threats, etc.). Optional services shall be itemized with description of functionality provided.

3.4. Qualifications

The Consultant is to have been regularly engaged in providing IT Managed Security Services as described in this RFP for a minimum period of five (5) years.

3.5. Security and Confidentiality

The Contractor will be required to complete and submit the City's Non-Disclosure Agreement.

All data or information is to be stored on servers inside Canada.

3.6. Billing and Reporting

A sample 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.

In addition, provide details of any electronic billing or reporting available to assist the City with management of the Services.

3.7. Co-Termination and Contract End Date

The Services will end on the expiry of the 3 year or 5-year term, calculated from the execution date of the Contract. ("End Date")
All Services, SLA's, and any other agreements, licensing etc. recommended or provided by the Consultant to perform the Services will terminate on the End Date. The City will not be responsible for any cancellation or early termination charges.

The Consultant will be responsible to manage the Co-Termination of products and services and will be solely responsible for any fees or charges past the Contract End Date

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

(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.

PROPOSAL SUBMISSION FORM

Complete and return this Proposal Submission Form - along with:

☐ Sample Invoice attached
☐ Financial Statements 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 an audited copy of their financial statements for the past three (3) years:

Attached to Proposal Submission:

☐ Yes ☐ No

If No, explain:

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:	