Request for Proposal ("RFP")

Canadian Commercial Corporation ("CCC")

Managed Security Services ("MSS") for
Security Incident Event Management ("SIEM") and
Security Operations Centre ("SOC")

CCC Reference No. 106205.138

Issued:
August 22, 2023

Questions to be received by CCC no later than:
2:00 PM Ottawa time
September 6, 2023 ("Question Period)

Submissions to be received by CCC no later than:
2:00 PM OTTAWA TIME
September 20, 2023 ("SUBMISSION DEADLINE")

Table of Contents

SECTION 1 – INVITATION AND SUBMISSION INSTRUCTIONS

1.1 Invitation

This Request for Proposals (the "RFP") is an invitation by the Canadian Commercial Corporation ("CCC") to prospective proponents to submit proposals for the supply and delivery of Managed Security Services (MSS) for SIEM (Security Incident Event Management) and SOC (Security Operations Centre) for all CCC assets on-premise and cloud-based assets as further described in Appendix A - Statement of Deliverables ("Deliverables").

The Canadian Commercial Corporation (CCC) is a federal Crown corporation and will be the source of funds for this project. Established in 1946, the Canadian Commercial Corporation is a federal Crown corporation of the Government of Canada established for the purpose of assisting in the development of trade between Canada and other nations.

The goal of this Managed Security Services RFP is to engage a reputed service provider organization that will be responsible for the management of SIEM services via a Security Operation Centre on a 24x7x365 basis. To be engaged on a one-year term with the option of renewing on a year-by-year basis, set out in Appendix A (RFP Particulars).

1.2 Proponent must be Single Entity

The proponent must be a single legal entity that, if selected, intends to negotiate and enter into the contract with CCC. If the proposal is being submitted jointly by two (2) or more separate entities, the proposal must identify only one of those entities as the "proponent". The proponent will be responsible for the performance of the Deliverables.

1.3 RFP Contact

For the purposes of this procurement process, the "RFP Contact" will be:

Canadian Commercial Corporation
350 Albert Street, Suite 700
Ottawa, Ontario K1A 0S6
Kathleen Nash, Contract Manager, Sourcing
Email: Bids@ccc.ca

Proponents and their representatives are not permitted to contact any employees, officers, agents, elected or appointed officials, or other representatives of CCC, other than the RFP Contact, concerning matters regarding this RFP. Failure to adhere to this rule may result in the disqualification of the proponent and the rejection of the proponent's proposal.

1.4 Contract for Deliverables

1.4.1 Type of Contract

The selected proponent will be requested to enter into contract negotiations to finalize an agreement with CCC for the provision of the Deliverables. The selected proponent will provide its terms and conditions for review as the basis for commencing negotiations between CCC and the selected proponent.

1.4.2 Term of Contract

The term of the contract will be for one year with the option to renew annually or to cancel 30 days prior to commencement of the new period. The vendor will be required to send a notification of the renewal least 60 days before the commencement of the new period.

1.5 RFP Timetable

1.5.1 Key Dates

The RFP timetable below is tentative only and may be changed by CCC at any time.

Issue Date of RFP	August 22, 2023
Deadline for Questions	September 6, 2023– 2:00 PM Ottawa time
Deadline for Issuing Addenda	September 13, 2023
Submission Deadline	September 20, 2023– 2:00 PM Ottawa time
Rectification Period	3 working days from notification
Anticipated Ranking of Proponents	October 4, 2023
Contract Negotiation Period	5 working days
Anticipated Execution of Agreement	October 25, 2023

1.6 Submission Instructions

1.6.1 Submission of Proposals

Proposals must be submitted by email to: BIDS@CCC.CA

The complete proposal must be received in the above-noted email inbox by the Submission Deadline. The time stamp of CCC's email system will be the official time for receipt of the proposal. Proposals received after the Submission Deadline may not be considered.

Proposals are to be submitted in PDF format and the email subject line should reference the RFP title and number (see RFP cover page).

Proponents should submit their proposals in two separate files.

1) Technical Proposal: One file should include the technical component of the proposal ("Technical Proposal") that should consist of the non-price rated requirements as described in Table 1 of Appendix B (Evaluation Criteria).
   - Naming Convention: VendorName – RFP 106205.138-Security-Technical Proposal

2) Price Proposal: One file should include the price proposal ("Price Proposal"), which should consist of:
   a. a fully completed and signed Submission Form (Appendix C) and
   b. a Pricing Table as set out by the proponent.
   - Naming Convention: VendorName – RFP 106205.138-Security-Price Proposal

Electronic submissions must not exceed 75 MB including email signature. Proponents should divide their responses into appropriately sized (smaller than 75 MB) numbered files. In the email the proponent should provide the details of each attachment and if there is more than one email. Proposals are stored in an electronically secure and restricted environment. Proposals will not be opened until after the Submission Deadline has passed.

1.6.2 Proposals to be Submitted on Time

Proposals must be received on or before the Submission Deadline set out in the title page of the RFP and as also set out in Article 1.5.1 (Key Dates).

Sending large documents via email may take significant time, depending on the file size and internet connection speed. It is strongly recommended that proponents allow sufficient time of at least one (1) hour before the Submission Deadline to send documents.

1.6.3 Amendment of Proposals

Proponents may amend their proposals prior to the Submission Deadline by submitting the amendment by email as above prominently marked with the RFP title and number to the email address set out above. Any amendment should clearly indicate which part of the proposal the amendment is intended to amend or replace.

1.6.4 Withdrawal of Proposals

At any time throughout the RFP process until the execution of a written agreement for provision of the Deliverables, a proponent may withdraw its proposal. To withdraw a proposal, a notice of withdrawal must be sent to the RFP Contact. CCC is under no obligation to return withdrawn proposals.

END OF SECTION 1

SECTION 2 – EVALUATION, NEGOTIATION AND AWARD

2.1 Stages of Evaluation and Negotiation

CCC will conduct the evaluation of proposals and negotiations in the following stages:

2.2 Stage I – Mandatory Submission Requirements

N/A

2.3 Stage II – Evaluation

2.3.1 Mandatory Technical Requirements

N/A

2.3.2 Non-Price Rated Criteria

The Technical Proposal is worth 100 of points out of 200 or 50% of the total score.

CCC will evaluate each qualified proposal on the basis of the non-price rated criteria as set out in Table 1 of the Appendix B (Evaluation Criteria).

The responses will be assessed on its appropriateness, completeness, and clarity in relation to the requirement (Appendix B). CCC will assign points for each criterion based on the points shown in each section of Table 1 of the Appendix B based on the scale in Chart 1 (Scale for Rating) below to determine the technical score.

Chart 1 – Scale for Rating	
Points	**Points Description**
0%	Barely addresses any of the stated requirements and completely lacking in critical areas.
30%	Adequately meets most of the stated requirements. May be lacking in some areas which are not critical.
50%	Meets most stated requirements
70%	**Meets all stated requirements**
80%	Meets all stated requirements and may exceed some
100%	Exceeds the stated requirements in superlative and beneficial ways.

In their Technical Proposal, respondents should address each criterion included in Table 1 of Appendix B clearly and in sufficient depth to permit a complete analysis and assessment by the evaluation team. The respondent's Technical Proposal should address each of the criteria in the order in which they appear and use the headings and numbering system of Table 1 in Appendix B.

Simply repeating the statement contained in the RFP is not sufficient. Respondents are requested to provide supporting data (reviews, examples, descriptions, lists, etc) to demonstrate their capability. If the respondent does not address a rated criterion the score for that rated criterion may be zero.

Chart 2 (Weighting of Points) below summarizes the categories, weightings, and descriptions of the rated evaluation criteria of the RFP. Respondents who do not meet the minimum threshold score for any category as shown in the chart below will not proceed to the next stage of the evaluation process.

Chart 2 – Weighting of Points			
ITEM	**RATED CRITERIA CATEGORY**	**WEIGHTING (POINTS)**	**MINIMUM THRESHOLD**
	Stage II - Evaluation of Non-Price Rated Criteria	50%	At least 50% on each criterion
1	Respondent's Organization	10 points	5 points
2	Experience – Relevant Examples (10 points each)	30 points	15 points
3	Experience – Key Team Members of Incident Response Team	20 points	10 points
4	Approach & Methodology	30 points	15 points
5	Work Plan	10 points	5 points
6	**Total - Technical Score**	**100 points**	**70% of total points (70 points)**
Minimum Threshold required 70 of 100 points to move forward to evaluation of Pricing			
	Stage III - Price Evaluation	50%	
7	Pricing on Managed Services (SIEM/SOC)	80 points	N/A
8	Pricing on incident response events	20 points	N/A
10	**Pricing Score**	**100 points**	**N/A**
11	**TOTAL SCORE (Item 6 & 10)**	**200 points**	**N/A**

2.4 Stage III – Pricing

2.4.1 Pricing – General

Stage III will consist of a scoring of the submitted pricing of each qualified proposal in accordance with the price evaluation method set out below to determine a pricing score ("Pricing Score"). The evaluation of price will be undertaken after the evaluation of mandatory requirements and rated criteria have been completed.

2.4.2 Pricing Evaluation

The Pricing Proposal is worth 100 points of the total score of 200 or 50% of total score.

The Pricing Score will be calculated based on a relative pricing formula. Each respondent will receive a percentage of the total possible points allocated to price, which will be calculated in accordance with the following formula:

$$lowest\ price \div respondent's\ price\ \times\ total\ points = respondent's\ pricing\ points$$

Example: Assume that there are two qualified bids, bid 'A' with a total price of $300,000 and bid "B" with a total price of $ 400,000. The lowest qualified bid "A" of $ 300,000 would receive 100 points. Bid "B" would receive:

= $300,000 ÷ $400,000 x 100 points
= 0.75 x 100 points
= 75 points

2.4.3 Instructions on How to Provide Required Pricing Information

(a) Proponents should submit their pricing information in a format suitable to the bid and include it in their proposals.

(b) Pricing must be provided in Canadian funds, inclusive of all applicable duties and taxes except for HST, which should be itemized separately.

(c) Unless otherwise indicated in the requested pricing information, prices quoted by the respondent must be all-inclusive and must include all labour and material costs, all travel and carriage costs, all insurance costs, all costs of delivery, all costs of installation and set-up, including any pre-delivery inspection charges, and all other overhead, including any fees or other charges required by law.

(d) All prices quoted must be firm, not-to-exceed amounts for the duration of the Agreement.

2.5 Stage IV – Ranking and Contract Negotiations

2.5.1 Ranking of Proponents

After the completion of Stage III, all scores from Stage II and Stage III will be added together and the proponents will be ranked based on their total scores. The top-ranked proponent will receive a written invitation to enter into contract negotiations to finalize the agreement with CCC. In the event of a tie, the selected proponent will be the proponent with the highest score on the non-price rated criteria.

2.5.2 Contract Negotiation Process

Any negotiations will be subject to the process rules contained in the Terms and Conditions of the RFP Process (Section 3) and will not constitute a legally binding offer to enter into a contract on the part of CCC or the proponent, and there will be no legally binding relationship created with any proponent prior to the execution of a written agreement. Negotiations may include requests by CCC for supplementary information from the proponent to verify, clarify, or supplement the information provided in its proposal or to confirm the conclusions reached in the evaluation, and may include requests by CCC for improved pricing or performance terms from the proponent.

2.5.3 Time Period for Negotiations

CCC intends to conclude negotiations and finalize the agreement with the top-ranked proponent during the Contract Negotiation Period, commencing from the date CCC invites the top-ranked proponent to enter negotiations. The proponent invited to enter into direct contract negotiations, may be require to satisfy the pre-conditions listed in 2.6 below, provide requested information in a timely fashion and conduct its negotiations expeditiously.

2.5.4 Failure to Enter into Agreement

If the pre-conditions of award listed in 2.6 below are not satisfied or if the parties cannot conclude negotiations and finalize the agreement for the Deliverables within the Contract Negotiation Period, CCC may discontinue negotiations with the top-ranked proponent and may invite the next-best-ranked proponent to enter into negotiations. This process will continue until an agreement is finalized, until there are no more proponents remaining that are eligible for negotiations, or until CCC elects to cancel the RFP process.

2.5.5 Notification of Negotiation Status

Other proponents that may become eligible for contract negotiations may be notified at the commencement of the negotiation process with the top-ranked proponent.

2.6 Stage VI – Pre-Conditions

2.6.1 Financial Capacity

Once the top-ranked respondent has been selected, and in order for the top-ranked respondent to demonstrate its financial capacity to successfully complete the project, the top-ranked respondent may be required to submit any financial information requested by CCC, within five (5) business days following CCC's request. Failure to provide the requested financial information within the required timeframe may result in the disqualification of the top-ranked respondent. If the requested financial information does not sufficiently demonstrate the top-ranked respondent’s financial capacity to successfully complete the project at CCC’s sole and absolute discretion, CCC

may request additional information, guarantees and/or securities. It will be at CCC's sole and absolute discretion to determine if the top-ranked respondent has demonstrated its financial capacity to successfully deliver the Deliverables, and if they have not, CCC may disqualify the top-ranked respondent. CCC will permit the top-ranked respondent to make representations prior to making a final decision to reject the proposal on these grounds. Such representation must be made within ten (10) days of CCC informing the respondent that it is considering such disqualification.

2.6.2 Security Assessment

Once the top-ranked respondent has been selected, CCC will perform its security assessment of the respondent. The top-ranked respondent will be asked to complete the CCC Security Assessment found in Appendix D (CCC's Security Assessment Form). Failure to provide the requested security assessment within five (5) business days will result in the disqualification of the respondent. If the security assessment does not sufficiently demonstrate the top-ranked respondent's security capacity, CCC may request additional information to clarify the responses made by the respondent, and if they have not, CCC may disqualify the top-ranked respondent. CCC will permit the top-ranked respondent to make representations prior to making a final decision to reject the proposal on these grounds. Such representations must be made within five (5) days of CCC informing the respondent that it is considering such disqualifications.

END OF SECTION 2

SECTION 3 – TERMS AND CONDITIONS OF THE RFP PROCESS

3.1 General Information and Instructions

3.1.1 Proponents to Follow Instructions

Proponents should structure their proposals in accordance with the instructions in this RFP. Where information is requested in this RFP, any response made in a proposal should reference the applicable section numbers of this RFP.

A proponent who submits conditions, options, variations, or contingent statements either as part of its proposal or after receiving notice of selection, may be disqualified.

3.1.2 Proposals in English or French

All proposals are to be in English or French only.

3.1.3 No Incorporation by Reference

The entire content of the proponent's proposal should be submitted in a fixed format, and the content of websites or other external documents referred to in the proponent's proposal but not attached will not be considered to form part of its proposal.

3.1.4 Past Performance

In the evaluation process, CCC may consider the proponent's past performance or conduct on previous contracts with CCC or other institutions.

3.1.5 Information in RFP Only an Estimate

CCC and its advisers make no representation, warranty, or guarantee as to the accuracy of the information contained in this RFP or issued by way of addenda. Any quantities shown or data contained in this RFP or provided by way of addenda are estimates only, and are for the sole purpose of indicating to proponents the general scale and scope of the Deliverables. It is the proponent's responsibility to obtain all the information necessary to prepare a proposal in response to this RFP.

3.1.6 Proponents to Bear Their Own Costs

The proponent will bear all costs associated with or incurred in the preparation and presentation of its proposal, including, if applicable, costs incurred for interviews or demonstrations.

3.1.7 Proposal to be Retained by CCC

CCC will not return the proposal or any accompanying documentation submitted by a proponent.

3.1.8 No Guarantee of Volume of Work or Exclusivity of Contract

CCC makes no guarantee of the value or volume of work to be assigned to the successful proponent. The agreement to be negotiated with the selected proponent will not be an exclusive contract for the provision of the described Deliverables. CCC may contract with others for goods and services the same as or similar to the Deliverables or may obtain such goods and services internally.

3.2 Communication after Issuance of RFP

3.2.1 Proponents to Review RFP

Proponents should promptly examine all of the documents comprising this RFP and may direct questions or seek additional information in writing by email to the RFP Contact on or before the Deadline for Questions. No such communications are to be sent or initiated through any other means. CCC is under no obligation to provide additional information, and CCC is not responsible for any information provided by or obtained from any source other than the RFP Contact. It is the responsibility of the proponent to seek clarification on any matter it considers to be unclear. CCC is not responsible for any misunderstanding on the part of the proponent concerning this RFP or its process.

CCC will only post information on CanadaBuys (https:// https://canadabuys.canada.ca/en) and is not responsible for information on any other websites.

3.2.2 All New Information to Proponents by Way of Addenda

This RFP may be amended only by addendum in accordance with this section. If CCC, for any reason, determines that it is necessary to provide additional information relating to this RFP, such information will be communicated to all proponents by addendum. Each addendum forms an integral part of this RFP and may contain important information, including significant changes to this RFP. Proponents are responsible for obtaining all addenda issued by CCC.

CCC will only post information on CanadaBuys (https:// https://canadabuys.canada.ca/en) and is not responsible for information on any other websites.

3.2.3 Post-Deadline Addenda and Extension of Submission Deadline

If CCC determines that it is necessary to issue an addendum after the Deadline for Issuing Addenda, CCC may extend the Submission Deadline for a reasonable period of time.

3.2.4 Verify, Clarify, and Supplement

When evaluating proposals, CCC may request further information from the proponent or third parties in order to verify or clarify the information provided in the proponent's proposal. CCC may revisit, re-evaluate, and rescore the proponent's response or ranking on the basis of any such information.

3.3 Notification and Debriefing

3.3.1 Notification to Other Proponents

Once an agreement is executed by CCC and a proponent, the other proponents may be notified directly in writing and will be notified by public posting of the outcome of the procurement process.

3.3.2 Debriefing

Proponents may request a debriefing after receipt of a notification of the outcome of the procurement process. All requests must be in writing to the RFP Contact and must be made within thirty (30) days of such notification. The RFP Contact will contact the proponent's representative to schedule the debriefing. Debriefings may occur in person at CCC's location or by way of conference call or other remote meeting format as prescribed by CCC.

3.4 Conflict of Interest and Prohibited Conduct

3.4.1 Conflict of Interest

For the purposes of this RFP, the term "Conflict of Interest" includes, but is not limited to, any situation or circumstance where:

(a) in relation to the RFP process, the proponent has an unfair advantage or engages in conduct, directly or indirectly, that may give it an unfair advantage, including but not limited to:

(i) having or having access to confidential information of CCC in the preparation of its proposal that is not available to other proponents;

(ii) having been involved in the development of the RFP, including having provided advice or assistance in the development of the RFP;

(iii) receiving advice or assistance in the preparation of its response from any individual or entity that was involved in the development of the RFP;

(iv) communicating with any person with a view to influencing preferred treatment in the RFP process (including but not limited to the lobbying of decision makers involved in the RFP process); or

(v) engaging in conduct that compromises, or could be seen to compromise, the integrity of the open and competitive RFP process or render that process non-competitive or unfair;

(b) in relation to the performance of its contractual obligations under a contract for the Deliverables, the proponent's other commitments, relationships, or financial interests:

(i) could, or could be seen to, exercise an improper influence over the objective, unbiased, and impartial exercise of its independent judgement; or

(ii) could, or could be seen to, compromise, impair, or be incompatible with the effective performance of its contractual obligations.

3.4.2 Disqualification for Conflict of Interest

CCC may disqualify a proponent for any conduct, situation, or circumstances, determined by CCC, in its sole and absolute discretion, to constitute a Conflict of Interest as defined above.

An existing supplier of CCC may be precluded from participating in the RFP process in instances where the CCC has determined that the supplier has a competitive advantage that cannot be adequately addressed to mitigate against unfair advantage. This may include, without limitation, situations in which an existing supplier is in a position to create unnecessary barriers to competition through the manner in which it performs its existing contracts, or situations where the incumbent fails to provide the information within its control or otherwise engages in conduct obstructive to a fair competitive process.

3.4.3 Disqualification for Prohibited Conduct

CCC may disqualify a proponent, rescind an invitation to negotiate, or terminate a contract subsequently entered into if CCC determines that the proponent has engaged in any conduct prohibited by this RFP.

3.4.4 Prohibited Proponent Communications

Proponents must not engage in any communications that could constitute a Conflict of Interest and should take note of the Conflict of Interest declaration set out in the Submission Form (Appendix C).

3.4.5 Proponent Not to Communicate with Media

Proponents must not at any time directly or indirectly communicate with the media in relation to this RFP or any agreement entered into pursuant to this RFP without first obtaining the written permission of the RFP Contact.

3.4.6 No Lobbying

Proponents must not, in relation to this RFP or the evaluation and selection process, engage directly or indirectly in any form of political or other lobbying whatsoever to influence the selection of the successful proponent(s).

3.4.7 Illegal or Unethical Conduct

Proponents must not engage in any illegal business practices, including activities such as bid-rigging, price-fixing, bribery, fraud, coercion, or collusion. Proponents must not engage in any unethical conduct, including lobbying, as described above, or other inappropriate communications; offering gifts to any employees, officers, agents, elected or appointed officials, or other representatives of CCC; deceitfulness; submitting proposals containing misrepresentations or other misleading or inaccurate information; or any other conduct that compromises or may be seen to compromise the competitive process provided for in this RFP.

3.4.8 Supplier Suspension

CCC may suspend a supplier from participating in its procurement processes for prescribed time periods based on past performance or based on inappropriate conduct, including but not limited to the following:

(a) illegal or unethical conduct as described above;

(b) the refusal of the supplier to honour its submitted pricing or other commitments;

(c) engaging in litigious conduct, bringing frivolous or vexatious claims in connection with CCC's procurement processes or contracts, or engaging in conduct obstructive to a fair competitive process; or

(d) any conduct, situation, or circumstance determined by CCC, in its sole and absolute discretion, to have constituted an undisclosed Conflict of Interest.

In advance of a decision to suspend a supplier, CCC will notify the supplier of the grounds for the suspension and the supplier will have an opportunity to respond within a timeframe stated in the notice. Any response received from the supplier within that timeframe will be considered by CCC in making its final decision.

3.5 Confidential Information

3.5.1 Confidential Information of CCC

All information provided by or obtained from CCC in any form in connection with this RFP either before or after the issuance of this RFP

(a) is the sole property of CCC and must be treated as confidential;

(b) is not to be used for any purpose other than replying to this RFP and the performance of any subsequent contract for the Deliverables;

(c) must not be disclosed without prior written authorization from CCC; and

(d) must be returned by the proponent to CCC immediately upon the request of CCC.

3.5.2 Confidential Information of Proponent

A proponent should identify any information in its proposal or any accompanying documentation supplied in confidence for which confidentiality is to be maintained by CCC. The confidentiality of such information will be maintained by CCC, except as otherwise required by law or by order of a court or tribunal. Proponents are advised that their proposals will, as necessary, be disclosed, on a confidential basis, to advisers retained by CCC to advise or assist with the RFP process, including the evaluation of proposals. If a proponent has any questions about the collection and use of personal information pursuant to this RFP, questions are to be submitted to the RFP Contact.

3.6 Procurement Process Non-Binding

3.6.1 No Contract A and No Claims

This procurement process is not intended to create and will not create a formal, legally binding bidding process and will instead be governed by the law applicable to direct commercial negotiations. For greater certainty and without limitation:

(a) this RFP will not give rise to any Contract A–based tendering law duties or any other legal obligations arising out of any process contract or collateral contract; and

(b) neither the proponent nor CCC will have the right to make any claims (in contract, tort, or otherwise) against the other with respect to the award of a contract, failure to award a contract or failure to honour a proposal submitted in response to this RFP.

3.6.2 No Contract until Execution of Written Agreement

This RFP process is intended to identify prospective suppliers for the purposes of negotiating potential agreements. No legal relationship or obligation regarding the procurement of any good or service will be created between the proponent and CCC by this RFP process until the successful negotiation and execution of a written agreement for the acquisition of such goods and/or services.

3.6.3 Non-Binding Price Estimates

While the pricing information provided in proposals will be non-binding prior to the execution of a written agreement, such information will be assessed during the evaluation of the proposals and the ranking of the proponents. Any inaccurate, misleading, or incomplete information, including withdrawn or altered pricing, could adversely impact any such evaluation or ranking or the decision of CCC to enter into an agreement for the Deliverables.

3.6.4 Cancellation

CCC may cancel or amend the RFP process without liability at any time.

3.7 Governing Law and Interpretation

These Terms and Conditions of the RFP Process (Section 3):

(a) are intended to be interpreted broadly and independently (with no particular provision intended to limit the scope of any other provision);

(b) are non-exhaustive and will not be construed as intending to limit the pre-existing rights of the parties to engage in pre-contractual discussions in accordance with the common law governing direct commercial negotiations; and

(c) are to be governed by and construed in accordance with the laws of the province of Ontario and the federal laws of Canada applicable therein.

END OF SECTION 3

APPENDIX A – RFP PARTICULARS

1. BACKGROUND

Canadian Commercial Corporation (CCC) is a Crown corporation (government-owned enterprise) established in 1946 under the *Canadian Commercial Corporation Act* and are accountable to the Parliament of Canada through the Minister of International Trade, Export Promotion, Small Business and Economic Development.

As the only Canadian agency that offers international contracting expertise to forge commercial contracts between Canadian businesses and foreign governments, we operate at the crossroads of commerce and international relations and enable Canadians to compete successfully in complex and highly competitive government procurement markets.

For more information about CCC, visit https://www.ccc.ca/en/about/

2. OBJECTIVES

CCC is seeking quotes from qualified vendors to provide Managed Security Services (MSS) for SIEM (Security Incident Event Management) and SOC (Security Operations Centre) for all CCC assets on-premises as well as cloud-based assets.

The goal of this Managed Security Services RFP is to engage a reputed service provider organization that will be responsible for the management of SIEM services via a Security Operation Centre on a 24x7x365 basis. To be engaged on a one-year term with the option of renewing on a year-by-year basis.

The main drivers are as follows:

a) Improve visibility and eliminate gaps in security through management of SIEM services via a Security Operation Centre on a 24x7x365 basis;
b) Comply with CCC Security Policies and standards as part of the overall information security risk management strategy. Policies to be provided to the Successful Bidder;
c) Comply with the Government of Canada's Direction to keep data residency in Canada. (see https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/direction-electronic-data-residency.html)
d) Provide Dark Web Hunting Services; and
e) Provide Digital Incident Response and Forensic Services.

3. SCOPE OF WORK

3.1 The Successful Bidder will provide a cloud-based system and all tools required to host and manage the SIEM/SOC solution.

3.2 The Successful Bidder must have Certified Forensic Team.

3.2 Requirements includes managed security services, more fully described in Article 4 (Service and Deliverables) around the devices that are listed in Schedule 1 to Appendix A (List of Key CCC Devices and Critical Applications), including but not limited to:

- Processing CCC log sources to identify all security incident events as more fully described in Article 4;
- Onboarding, storing, analyzing, correlating, and assessing the security incident events;
- Informing CCC immediately for further investigation and remediation of incidents;
- Providing regular reporting on findings and working with CCC team to provide recommendations;
- Upon request, assisting CCC to investigate logs of the potential incidents;
- Incident response services, including remediation of any security incidents;

- Maintenance of CCC logs for a minimum of 3 months online and for a minimum of one year offline; and
- Dark web hunting.

3.3 The Successful Bidder is expected to continually optimize and tune the SIEM to reduce false positives.

3.4 The Successful Bidder will also work with CCC to plan and provide a Yearly Penetration Test.

4. SERVICES AND DELIVERABLES

4.1 Responsibility Matrix

a) Service Element: Hardware and Software	CCC Responsibility	Successful Bidder Responsibility
Supply and install SIEM Hardware and Software in Successful Bidder's private cloud		Yes
Install and configure SIEM Software		Yes
Provide integration with CCC Team Dynamix central ticketing system.		Yes
Provide Security Operating Centre (SOC) phone number as a single point of contact for CCC		Yes
Permit and provide remote access to Successful Bidder to allow it to monitor and support	Yes	
Backup Service configuration once daily	Support	Yes

b) Service Element: Log Collection & Retention	CCC Responsibility	Successful Bidder Responsibility
Installation, implementation, configuration, troubleshooting and removal of the supported log collector software.	Support	Yes
Monitor monitored log sources and respond to all potential service incidents that may affect acquisition of logs from them.		Yes
Ensure network connectivity and performance for the managed log collector agents to the service	Yes	Support

c) Service Element: Use Cases & Alerting	CCC Responsibility	Successful Bidder Responsibility
Define and maintain alerting use case handling instructions, including priority level, automated handling, analyst investigative procedures, escalation policy, and CCC contact details.	Support	Yes

Security Monitoring Services: • Automated analytics of logs as per established use cases • Automated alerting and reporting as an output of established use cases • Provide recommendations on required log type to support security operations (the SIEM solution and the services) and requested/established use cases • Evaluation of the alert validity and risk indicated (qualification) as per agreed handling process • Guide use case tuning through alert handling and meeting interactions, and execute tuning through service request • Gather supporting evidence (logs) • Send security alert to CCC with context (as per agreed handling process) within the required timelines • Provide supporting data and evidence (logs) to help CCC understand and respond to the security alert • Create, maintain and tune use cases ongoing basis to improve visibility	Support	Yes
Monthly summary reports of *alerting use case* and identified issues. Quarterly summary report including analytics on log data in addition to monthly summary report metrics, accompanied by in-person / virtual review meeting.		Yes Yes

4.2 Hardware and Software Service Level Agreements (SLA)

Summary of Requirements	Requirement Details	Associated SLA
Install and configure SIEM software and provide access to CCC to view dashboard and current activities and history	Target service availability of 99.9% for the private cloud SIEM solution.	It excludes infrastructure related outages, including networking that is managed by the CCC. Successful Bidder will only start billing once onboarding and basic alerting is completed. Successful Bidder will make reasonably commercial efforts to complete installation in 45 days following the signing of the contract. Delay to this timeline due to Successful Bidder issues will be deemed an SLA violation to this agreement.
Provide an integration with CCC Team Dynamics Incident Management system, provide SOC phone number as a single point of contact for CCC.	Successful Bidder will provide CCC with a single toll-free telephone number to contact the help desk. This service will be available 7x24x365.	Target service availability of 99.9% for the ticketing system and SOC number availability.
Monitor Monitored log sources and respond to all potential service incidents that may	Successful Bidder will remotely monitor logs being received by the SIEM solution. Successful Bidder will alert the CCC when devices stop sending logs to the SIEM solution.	Log stoppage from critical devices (as defined per expected log frequency per device) will be treated as P1 incident – critical severity as described below.

affect acquisition of logs from them.	Response time will be based on criticality of the devices. Criticality will be determined by the CCC.	
Use Cases & Alerting		
Security Monitoring Service	Successful Bidder has developed several correlated security alerts. These alerts are more complex and consider different type of events from different devices to trigger based on agreed threat scenarios with the CCC. The response to security alerts will again follow the security monitoring SLAs set out herein. Alternatively, the CCC use the ticketing system or the SOC phone number, or both to initiate a security event investigation.	Security monitoring SLA Successful Bidder will notify CCC upon investigation and categorization of security alerts following CCC's Incident response policy (can be provided upon request.)

5. TIMELINES

1) Installation of SIEM software. See timelines in SLA table in clause 4.2 above.
2) Begin regular SIEM/SOC monthly services once installation is complete.
3) Begin Incident Response On-boarding.

6. TRAVEL EXPENSES

No travel is expected.

7. USE OF SUBCONTRACTORS

CCC requires Bidders to confirm whether they will provide the services identified in these Deliverables with their own employees or through subcontracting the work to a third party.

Schedule 1 to Appendix A

List of Key CCC Devices & Critical Applications.

ITEM	**Count (approx)**
Windows Servers	40-50 Virtual Machines
Linux Servers	5 Virtual Machines; 10 physical appliances
Physical Windows Servers	1 HP Proliant Hardware
Physical ESX Hypervisor Servers	2 Production / 2 Test – HP Proliant Hardware
Clustered Firewalls	1
VPN Appliances	1 (built into firewall)
Load Balancers	0
Domain Controllers	2
Databases	3 SQL Servers (1 Prod; 2 Test)
Application Servers - Windows	10 Critical
M365 - Office 365	1 Production tenant with E5 Licensing, leveraging Exchange Online, Sharepoint, Teams, Defender, Endpoint Manager, Azure AD. MFA and conditional access policies in place, some Azure Enterprise Applications deployed and used internally.
Switches / Routers	6 Switches Stacked / 1 Router (Router managed by third party)
Total Endpoints	250

APPENDIX B – EVALUATION CRITERIA

Refer to Section 2 of the RFP for information on the method of evaluation.

NON-PRICE RATED EVALUATION CRITERIA	100 points
1. Respondent's Organization	**10 points**

Provide a description of your company's organization including the below noted items.

a) Provide a brief description of the background and organization of the company, including location of your headquarters.
b) Describe the size of the company.
c) Describe your areas of expertise.
d) Provide the number of years of expertise in this domain.
e) List any subcontractors being used.
f) Describe the capacity of the firm to support CCC's requirements.
g) List the names of similar Public Sector bodies or agencies for whom you currently provide similar services for in Canada.
h) List the number of existing clients you currently support and the countries they reside in.

2. Experience - Relevant Examples (10 points each)	**30 Points**

Respondents should concisely describe the relevant experience of the respondent in three (3) examples of similar scope and complexity as required by CCC, within the last three (3) years. Provide an example for each of the services identified below:

1) Security Management Services via SOC (Security Operations Centre) – provide an example of a security management service in action by describing the chain of escalation and the incident response framework/policy followed. Describe the communications and timeline. Demonstrate how standards such as NIST, PCI DSS, COBIT and SOC II are followed and achieved.
2) Security Incident Event Management – provide an example the SIEM identified an suspicious activity and describe the chain of response.
3) Digital Incident Response and Forensic Services – provide an example of when you and your team were the primary support for a client who experienced a Cyber Security incident. Describe remediation services and outcome of incident.

Respondents should follow the format of the table provided in Schedule 1 to Appendix B (Project Description Form), to respond to this Rated Requirement.

3. Experience - Key Team Members of Incident Response Team	20 Points

Identify key team members that are being proposed and concisely describe the following:

- Role and responsibilities; and
- Relevant education, accreditations, qualifications, and experience as it relates to cyber security and incident response.

Respondents should follow the format of the table provided in Schedule 2 to Appendix B (Key Team Member Description Form) to respond to this Rated Requirement. Provide a separate table for each proposed Key Team Member.

4. Approach & Methodology	**30 points**

Respondents should concisely describe the overall approach which outlines the respondent's strategies, assumptions and philosophies in providing the services contemplated in Appendix A (RFP Particulars).

Respondents should further address each of the following components and describe a comprehensive process for delivering these services, including any proposed innovative solutions:

- Security Operations Centre (SOC), including service level, activities, tools, standards, data warehousing, and reporting (preference will be given to data residency in Canada per Canadian Government Security Requirements).
- Security Incident Event Management (SIEM), including the methodology to continually optimize and tune the SIEM to increase effectiveness and reduce false positives and report on improvements.
- Digital Incident Response and Forensic Services, including any activities, tools, and reports.

5. Work Plan	**10 points**

Outline the plan for the implementation of service with detailed activities/tasks for the assignment, content, and duration. Also provide a schedule of events or activities for the ongoing services.

For the proposal to be technically acceptable, it must score a minimum of 70 points out of 100 points (Meets all stated requirements). A proposal that does not meet that score will be disqualified from the process.

Refer to Section 2 of the RFP for information on the method of evaluation.

Price Proposal Evaluation			**100 points**
1		Provide pricing on SIEM SOC Managed Services (24/7 SOC Monitoring).	60 points
2		Provide the cost for incident response.	20 points

Refer to Section 2.6 of the RFP for pre-conditions of award.

Schedule 1 to APPENDIX B

Example Description Form

Example Title:	
Client:	
Timeline of event:	
Overview	
Respondent's Roles and Responsibilities:	
Methodology:	
Complexity, identify any unique and relevant issues successfully addressed:	
Outcome:	

Schedule 2 to APPENDIX B

Key Team Members Description Form
Incident Response Team

Name	Role	Education & Accreditation	Qualifications & Experience	Years of Experience

APPENDIX C – SUBMISSION FORM
Digital Risk Monitoring and Protection Services

1. Proponent Information

Please fill out the following form, naming one person to be the proponent's contact for the RFP process and for any clarifications or communication that might be necessary.	
Full Legal Name of Proponent:	
Any Other Relevant Name under which Proponent Carries on Business:	
Street Address:	
City, Province/State:	
Postal Code:	
Phone Number:	
Company Website (if any):	
Proponent Contact Name and Title:	
Proponent Contact Phone:	
Proponent Contact Email:	

2. Acknowledgment of Non-Binding Procurement Process

The proponent acknowledges that the RFP process will be governed by the terms and conditions of the RFP, and that, among other things, such terms and conditions confirm that this procurement process does not constitute a formal, legally binding bidding process (and for greater certainty, does not give rise to a Contract A bidding process contract), and that no legal relationship or obligation regarding the procurement of any good or service will be created between CCC and the proponent unless and until CCC and the proponent execute a written agreement for the Deliverables.

3. Ability to Provide Deliverables

The proponent has carefully examined the RFP documents and has a clear and comprehensive knowledge of the Deliverables required. The proponent represents and warrants its ability to provide the Deliverables in accordance with the requirements of the RFP for the rates set out in its proposal.

4. Non-Binding Pricing

The proponent has submitted its pricing in accordance with the instructions in the RFP. The proponent confirms that the pricing information provided is accurate. The proponent acknowledges that any inaccurate, misleading, or incomplete information, including withdrawn or altered pricing, could adversely impact the acceptance of its proposal or its eligibility for future work.

5. Addenda

The proponent is deemed to have read and taken into account all addenda issued by CCC prior to the Deadline for Issuing Addenda.

6. Communication with Competitors

For the purposes of this RFP, the word "competitor" includes any individual or organization, other than the proponent, whether or not related to or affiliated with the proponent, who could potentially submit a response to this RFP.

Unless specifically disclosed below under Disclosure of Communications with Competitors, the proponent declares that:

(a) it has prepared its proposal independently from, and without consultation, communication, agreement or arrangement with any competitor, including, but not limited to, consultation, communication, agreement or arrangement regarding:

(i) prices;

(ii) methods, factors or formulas used to calculate prices;

(iii) the quality, quantity, specifications or delivery particulars of the Deliverables;

(iv) the intention or decision to submit, or not to submit, a proposal; or

(v) the submission of a proposal which does not meet the mandatory technical requirements or specifications of the RFP; and

(b) it has not disclosed details of its proposal to any competitor and it will not disclose details of its proposal to any competitor prior to the notification of the outcome of the procurement process.

Disclosure of Communications with Competitors

If the proponent has communicated or intends to communicate with one or more competitors about this RFP or its proposal, the proponent discloses below the names of those competitors and the nature of, and reasons for, such communications:

_____

_____

_____

_____

_____

_____

7. No Prohibited Conduct

The proponent declares that it has not engaged in any conduct prohibited by this RFP.

8. Conflict of Interest

The proponent must declare all potential Conflicts of Interest, as defined in section 3.4.1 of the RFP. This includes disclosing the names and all pertinent details of all individuals (employees, advisers, or individuals acting in any other capacity) who (a) participated in the preparation of the proposal; **AND** (b) were employees of CCC within twelve (12) months prior to the Submission Deadline.

If the box below is left blank, the proponent will be deemed to declare that (a) there was no Conflict of Interest in preparing its proposal; and (b) there is no foreseeable Conflict of Interest in performing the contractual obligations contemplated in the RFP.

Otherwise, if the statement below applies, check the box.

- ❑ The proponent declares that there is an actual or potential Conflict of Interest relating to the preparation of its proposal, and/or the proponent foresees an actual or potential Conflict of Interest in performing the contractual obligations contemplated in the RFP.

If the proponent declares an actual or potential Conflict of Interest by marking the box above, the proponent must set out below details of the actual or potential Conflict of Interest:

_____

_____

_____

9. Disclosure of Information

The proponent hereby agrees that any information provided in this proposal, even if it is identified as being supplied in confidence, may be disclosed where required by law or by order of a court or tribunal. The respondent hereby agrees that, for any Agreement resulting from this RFP, CCC will publicly disclose the following information:

(a) Description of the goods and services;
(b) The name and address of the parties;
(c) The date of award and Agreement period;
(d) The value of the Agreement;
(e) The reference number assigned to the Agreement, if any;
(f) The type of procurement method used, and in cases where limited tendering was used, a description of the circumstances justifying its use; and
(g) Any other information that, in accordance with the Treasury Board policies, must be published.

The proponent hereby consents to the disclosure, on a confidential basis, of this proposal by CCC to the advisers retained by CCC to advise or assist with the RFP process, including with respect to the evaluation of this proposal.

The proponent hereby agrees that CCC may release to the other proponents the name of the successful proponent and the total points obtained by the successful proponent. This condition is subject to the requirements of the Privacy Act and the name and score of an individual will be released only in accordance with the requirements of the Privacy Act. We further acknowledge and agree that we shall have no right to claim against CCC, its employees, agents or servants of the Crown, in relation to such disclosure of information.

10. Availability of Resources

We represent and warrant that the entities and persons proposed in the Proposal to perform the Deliverables will be the entities and persons that will perform the Deliverables in the fulfilment of the Project under any contractual arrangement arising from submission of the Proposal. Save for poor performance as determined by the proponent, changes to the project resources following contract award shall only be made if pre-approved by CCC for causes due to events beyond the control of the proponent, including: death, sickness, maternity and parental leave, retirement, resignation, dismissal for cause or termination of an agreement for default.

11. Proponent Declaration

The proponent declares that:

a. our proposal does not include delivery of goods that originate, either directly or indirectly, from entities listed, in relation to terrorist groups and those who support them, under subsection 83.05(1) of the Criminal Code of Canada, and identified thereto in a “List of Entities” which may be found at:

http://www.osfi-bsif.gc.ca/Eng/fi-if/amlc-clrpc/atf-fat/Pages/default.aspx or
http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cntr-trrrsm/lstd-ntts/crrnt-lstd-ntts-eng.aspx.

b. neither we nor any member of the proponent have, directly or indirectly, paid or agreed to pay, and will not, directly or indirectly, pay, a contingency fee to any individual for the solicitation, negotiation or obtaining of the Agreement if the payment of the fee would require the individual to file a return under section 5 of the *Lobbying Act*;

c. neither we nor any member of the proponent have been convicted of an offence or sanctioned within the last five (5) years under Section 239 of the *Income Tax Act* (Revised States of Canada, 1985, chapter 1, 5th Supplement), Section 327 of the *Excise Tax Act* (Revised States of Canada, 1985, Chapter E-15) or any equivalent or similar provision contained in a provincial statute;

d. neither we nor any member of the proponent have ever been convicted of an offence under Section 121 (Frauds on the government and Contractor subscribing to election fund), Section 124 (Selling or Purchasing Office), Section 380 (Fraud) or Section 418 (Selling defective stores to Her Majesty) of the *Criminal Code of Canada* (https://laws-lois.justice.gc.ca/eng/acts/c-46/), or under paragraph 80(1)(d) (False entry, certificate or return) subsection 80(2) (Fraud against Her Majesty), Section 154.01 (Fraud against Her Majesty) of the *Financial Administration Act* (https://laws-lois.justice.gc.ca/eng/acts/F-11/) or the *Corruption of Foreign Public Officials Act* (https://laws-lois.justice.gc.ca/eng/acts/c-45.2/);

e. neither we nor any member of the proponent have ever been convicted of an offence under any of the provisions referred to in subsection 750(3) of the *Criminal Code* or that, if the Respondent or any member of the proponent has been convicted of any of those offences, it is one for which

   i. a pardon was granted under the *Criminal Records Act* – as it read immediately before the coming into force of section 109 of the *Safe Streets and Communities Act* – that has not been revoked or ceased to have effect;

   ii. a record suspension has been ordered under the *Criminal Records Act* and that has not been revoked or ceased to have effect;

   iii. an order of restoration was made under sub-section 750(5) of the *Criminal Code* that restores the proponent's capacity to enter into the Agreement or to receive any benefit under the Agreement as the case may be; or

   iv. the conviction was set aside by a competent authority.

f. We have not been declared ineligible by Her Majesty or under Canadian laws, official regulations, or by an act of non-compliance with a decision of the United Nations Security Council, and we understand that in the event that any such circumstances arise we may be deemed ineligible for contract award.

Signature of Proponent Representative _____

Name of the Proponent Representative _____

Title of the Proponent Representative _____

Date _____

I have the authority to bind the proponent.

APPENDIX D – VENDOR SECURITY QUESTIONNAIRE

For reference purposes only. Do not complete unless you are requested to do so.

Vendor Name:	
Completed By:	Name of person responding
Date Completed:	

#	Question	Vendor Response	Vendor Comments
1	**Document Requests**		
1.1	Please attach a copy of your information security policy		
1.1	Please attach a copy of any information security or privacy certifications (e.g. ISO 27001, PCI DSS, GDPR)		
1.3	Please attach a copy of any relevant audit reports that cover information security controls (e.g. SOC 2)		
1.4	Please attach a copy of your latest penetration test and/or vulnerability assessment report		
2	**Asset Management**		
2.1	Do you maintain an inventory of all hardware and software assets, including ownership?		
2.2	Do you have an information classification scheme and process designed to ensure that information is protected according to its confidentiality requirements?		
2.3	Do you maintain an inventory or map of data flows between both internal and external information systems?		
3	**Governance**		
3.1	Do you have an information security policy that has been approved by management and communicated to all applicable parties?		
3.2	Do you have an information security policy exception process that includes formal acceptance of risk by the risk owner?		
3.3	Do you have a process for reviewing your information security policy at least biennially?		
3.4	Do you regularly perform security threat and risk assessments on critical information systems using an industry-standard risk assessment methodology?		
3.3	Have you designated an individual, who is at least at a manager level, who is responsible for information security activities?		
3.6	Do you have a process designed to monitor changes to regulations and ensure compliance with relevant security requirements?		
4	**Supply Chain Risk Management**		
4.1	Do you perform security assessments on potential suppliers prior to entering into agreements with them?		
4.2	Do your agreements with suppliers include appropriate measures designed to meet security requirements?		
4.3	Do you regularly evaluate suppliers to ensure that they are meeting their security obligations?		
5	**Identity Management, Authentication, and Access Control**		
5.1	Is all access to information systems formally approved by the appropriate asset owner?		
5.2	Can all access to information systems be traced to unique individuals?		
5.3	Are all access rights to information systems regularly reviewed for appropriateness by the asset owners?		
5.4	Are all access rights to information systems immediately revoked upon employee/contractor termination or change of role?		
5.5	Do you restrict and control the use of privileged accounts through the use of a Privileged Account Management system or equivalent controls?		
5.6	Do you manage access permissions and authorizations, incorporating the principles of least privilege and separation of duties?		
5.5	Do you require the use of multi-factor authentication for all remote access to organizational data, including email?		
5.6	Do you require the use of multi-factor authentication for all administrative access to cloud-based information systems?		
6	**Human Resource Security**		

6.1	Do you have an information security awareness program designed to ensure that all employees and contractors receive security education as relevant to their job function?		
6.2	Do you conduct regular phishing simulation tests of your employees?		
6.2	Do you conduct appropriate background checks on all new employees based on the sensitivity of the role that they are being hired for?		
.3	Do you require all new employees and contractors to sign confidentiality agreements?		
7	**Data Security**		
7.1	Do you require that all removable media, which may contain organizational data, is encrypted?		
7.2	Do you require that all media, including hardcopies, containing organizational data is disposed of securely when no longer required?		
7.3	Have you implemented data loss prevention tools?		
7.3	Do you employ full disk encryption on all laptops?		
7.5	Do you encrypt databases?		
8	**System Acquisition, Development, and Maintenance**		
8.1	Are information security requirements defined for all new information systems, whether acquired or developed?		
8.2	Are development and testing environments separate from the production environment?		
8.3	Is data used for development and testing protected through anonymization?		
8.4	Are information security requirements tested to ensure that they function as designed?		
8.5	Are your applications developed with secure coding practices, including the OWASP Top 10 Most Critical Web Application Security Risks?		
8.6	Are your web applications protected by an application layer firewall?		
8.7	Do you incorporate threat modeling into application design?		
8.6	Is application source code tested for vulnerabilities using source code reviews or static application security testing?		
8.7	Are new information systems scanned for vulnerabilities prior to deployment?		
8.10	Do you monitor and restrict the installation of unauthorized software?		
9	**Physical and Environmental Security**		
9.1	Data Residency- are all CCC data processed and stored in a data center located in Canada? This applies to all data backups and copies. Please add the name and location(s) of the used data center(s)		
9.2	Are physical security perimeter controls implemented around sensitive locations such as data centers?		
9.3	Are all visitors appropriately identified, logged, and escorted while in sensitive locations?		
10	**Information Protection Processes and Procedures**		
10.1	Are security configuration baselines defined and implemented for all endpoints and network devices?		
10.2	Do you use automated tools to verify that endpoints and network devices comply with their baselines?		
10.2	Do you segregate your network into zones based on trust levels, and control the flow of traffic between zones?		
10.3	Do you control the transfer of information to external parties through authentication and encryption?		
10.4	Are all changes to information systems recorded, planned, and tested?		
10.5	Are all information systems that are susceptible to malware protected by up-to-date anti-malware software?		
10.6	Do you have a backup and recovery process designed to ensure that data can be recovered in the event of unexpected loss?		
10.7	Do you segregate wireless network access for BYOD and guest access from your production network?		
10.8	Do you enforce containerization on all mobile devices that may contain organizational data, including email, whether those devices are owned by the organization or by employees?		
10.10	Do you have the capability of deleting all organizational data from mobile devices, whether owned by the organization or by employees, in the event that the device is lost or stolen?		

10.9	Do you monitor external sources, such as vendor bulletins, for newly identified vulnerabilities and patches?		
10.10	Do you evaluate, test, and apply information system patches in a timely fashion according to their risk?		
11	**Protective Technology**		
11.1	Have security event logging requirements been defined, and are all information systems configured to meet logging requirements?		
11.2	Are security event logs protected and retained per defined logging requirements?		
11.3	Have you deployed intrusion detection or prevention systems at the network perimeter?		
11.4	Have you deployed tools to limit web browsing activity based on URL categories?		
11.4	Have you deployed controls to detect and mitigate denial of service attacks?		
12	**Security Continuous Monitoring**		
12.1	Have you deployed automated tools to collect, correlate, and analyze security event logs from multiple sources for anomalies?		
12.2	Do you monitor privileged user activity to detect potential security events?		
12.3	Do you monitor user activity to detect potential security events?		
12.4	Are security alerts monitored 24x7?		
12.3	Do you employ automated tools to scan information systems for vulnerabilities on a regular basis?		
12.6	Do you perform penetration tests on all web applications and services, in accordance with standard penetration testing methodologies?		
13	**Information Security Incident Management**		
13.1	Do you have a formal, documented security incident response plan?		
13.2	Do you conduct regular tests of your security incident response plan?		
13.3	Are all security incidents recorded, classified, and tracked?		
13.4	Are forensic investigations conducted as part of incident response?		
14	**Privacy**		
14.1	Do you have a data retention policy and process that is designed to meet relevant privacy regulations?		
14.2	Do you maintain an inventory and mapping of where all personal data is stored that includes cross-border data flows?		