



**Cabinet Office and Digital Innovation**  
**Department of Information and Digital Technologies**

**Request for Proposals**  
**For**  
**Managed Detection and Response Services**  
**(Restricted Request For Proposals)**

Request for Proposals No.: **BDA-CAB-IDT-SECURITY-2026-04**

Issued: **Friday April 24, 2026**

Submission Deadline: **Thursday May 21, 2026 05:00:00 PM Bermuda Local Time**

## TABLE OF CONTENTS

<b>PART 1 – INVITATION AND SUBMISSION INSTRUCTIONS.....</b>	<b>3</b>
1.1 Invitation to Proponents .....	3
1.2 RFP Contact.....	3
1.3 Type of Contract for Deliverables.....	3
1.4 RFP Timetable.....	4
1.5 Submission of Proposals .....	4
<b>PART 2 – EVALUATION, NEGOTIATION AND AWARD.....</b>	<b>6</b>
2.1 Stages of Evaluation and Negotiation .....	6
2.2 Stage I – Mandatory Submission Requirements .....	6
2.3 Stage II – Evaluation .....	6
2.4 Stage III – Pricing .....	6
2.5 Stage IV – Ranking and Contract Negotiations.....	6
<b>PART 3 – TERMS AND CONDITIONS OF THE RFP PROCESS.....</b>	<b>8</b>
3.1 General Information and Instructions .....	8
3.2 Communication after Issuance of RFP .....	9
3.3 Notification and Debriefing.....	10
3.4 Conflict of Interest and Prohibited Conduct.....	10
3.5 Confidential Information.....	12
3.6 Procurement Process Non-Binding.....	13
3.7 Governing Law and Interpretation.....	14
<b>APPENDIX A - FORM OF AGREEMENT .....</b>	<b>15</b>
<b>APPENDIX B – SUBMISSION FORM .....</b>	<b>16</b>
<b>APPENDIX C – PRICING .....</b>	<b>20</b>
<b>APPENDIX D – RFP PARTICULARS.....</b>	<b>22</b>
A. THE DELIVERABLES .....	22
B. MATERIAL DISCLOSURES.....	27
C. MANDATORY SUBMISSION REQUIREMENTS .....	29
D. MANDATORY TECHNICAL REQUIREMENTS.....	31
E. PRE-CONDITIONS OF AWARD .....	32
F. RATED CRITERIA .....	32
<b>APPENDIX E – CERTIFICATE OF CONFIRMATION OF NON-COLLUSION .....</b>	<b>34</b>
 ANNEX A - FORM OF AGREEMENT	
 ANNEX B - REQUIRED PRICING FORM	
 ANNEX C - COMPANY PROFILE FORM	
 ANNEX D - LOCAL BENEFITS	

# PART 1 – INVITATION AND SUBMISSION INSTRUCTIONS

## 1.1 Invitation to Proponents

This Request for Proposals (the “RFP”) is an invitation by the Government of Bermuda (the “Government”) to prospective proponents to submit proposals for **Managed Detection and Response Services** as further described in Section A of the RFP Particulars (Appendix D) (the “Deliverables”).

This RFP is restricted to the successful respondents of Request of Supplier Qualifications for Security Partner Project Number BDA-CAB-IDT-SECURITY-2025-04.

The Government of Bermuda is responsible for delivering critical services to the community and maintaining sensitive data across a variety of platforms and departments. The Government of Bermuda is held to high standards of transparency, accountability, and operational continuity. In an era of increasing cyber threats targeting government entities, ensuring the confidentiality, integrity, and availability of systems and information has become a mission-critical priority.

The Government of Bermuda is seeking proposals from an experienced cybersecurity service provider capable of supporting a comprehensive security strategy. This strategy will focus on strengthening both preventative and responsive capabilities—emphasizing strategic guidance, operational readiness, and the flexibility to evolve alongside emerging threats and technologies.

## 1.2 RFP Contact

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

Tiffany Tucker @ tintucker@gov.bm

Proponents and their representatives are not permitted to contact any employees, officers, agents, elected or appointed officials or other representatives of the Government, 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.

Prior to the Submission Deadline noted in the RFP timetable below, proponents that download this file and intend to respond to this RFP are required to register their interest with the RFP contact by emailing their company name and contact information to

Tiffany Tucker @ tintucker@gov.bm

Amendment/addenda (if any) will be posted at <https://www.gov.bm/procurement-notices>. Proponents should visit the Government Portal on a regular basis during the procurement process.

## 1.3 Type of Contract for Deliverables

The selected proponent will be requested to enter into direct contract negotiations to finalize an agreement with the Government for the provision of the Deliverables. The terms and conditions found in the Form of Agreement (Appendix A) are to form the basis for commencing negotiations between the Government and the selected proponent. It is the Government’s intention to enter into an agreement with only one (1) legal entity.

The term of the agreement is to be for a period of 3 years, with an option in favour of the Government to extend the agreement terms and conditions acceptable to the Government and the selected proponent for an additional term of up to 1 year. An Agreement is subject to change until fully executed.

Joint submissions are acceptable however, if a joint submission is made, the submission must clearly indicate which party will act as the prime contractor.

## **1.4 RFP Timetable**

### **1.4.1 Key Dates**

Issue Date of RFP	Friday April 24, 2026
No Pre-Bid / Site Meeting	
Deadline for Questions	Friday May 08, 2026
Deadline for Issuing Addenda	Friday May 15, 2026
Submission Deadline	Thursday May 21, 2026 05:00:00 PM
Rectification Period	5 business days
Anticipated Ranking of Proponents	Friday June 05, 2026
Contract Negotiation Period	30 calendar days
Anticipated Execution of Agreement	Wednesday June 17, 2026

All times listed are Bermuda local time. The RFP timetable is tentative only and may be changed by the Government at any time. For greater clarity, business days means all days that the Government is open for business.

### **1.4.2 Site Visit / Pre-Bid Meeting**

N/A

## **1.5 Submission of Proposals**

### **1.5.1 Proposals to be Submitted at Prescribed Location**

Electronic mail (E-Mail) submissions are accepted at [tintucker@gov.bm](mailto:tintucker@gov.bm)

### **1.5.2 Proposals to be Submitted on Time**

Proposals must be submitted at the location set out above on or before the Submission Deadline. Proposals submitted after the deadline will be rejected.

### **1.5.3 Proposals to be Submitted in Prescribed Format**

Proponents shall submit at minimum 0 original signed hard copies of their proposal or one (1) electronic copy (e-copy) in Microsoft Word or Adobe PDF format. If both a hard copy and an e-copy of the proposal are submitted and there is a conflict or inconsistency between the hard copy and the e-copy of the proposal, the hard copy of the proposal will prevail.

The original and all copies of the proposal shall be typed or written in indelible ink and shall be signed by a person duly authorized to sign on behalf of the Proponent. This authorization shall consist of a written authorization and shall be attached to the Submission Form included in (Appendix B). The name and position held by each person signing the authorization must be typed

or printed below the signature. An Electronic Record of Signature will be accepted in the submission only in accordance with the requirements laid out in the Electronic Transactions Act 1999. Any interlineation, erasures, or overwriting shall be valid only if they are signed or initialed by the person signing the proposal.

Proposals should be submitted in a sealed package and prominently marked with the RFP title and number (see RFP cover) and do not be opened until Thursday May 21, 2026 05:00:00 PM. The full legal name and return address of the proponent should be marked on the package as well.

#### **1.5.4 Amendment of Proposals**

Proponents may amend their proposals prior to the Submission Deadline by submitting the amendment in a sealed package prominently marked with the RFP title and number and the full legal name and return address of the proponent to the location set out above. Any amendment should clearly indicate which part of the proposal the amendment is intended to amend or replace.

#### **1.5.5 Withdrawal of Proposals**

At any time throughout the RFP process until the execution of a written agreement for the provision of the Deliverables, a proponent may withdraw a submitted proposal. To withdraw a proposal, a notice of withdrawal must be sent to the RFP Contact and must be signed by an authorized representative of the proponent. The Government is under no obligation to return withdrawn proposals.

[End of Part 1]

## **PART 2 – EVALUATION, NEGOTIATION AND AWARD**

### **2.1 Stages of Evaluation and Negotiation**

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

### **2.2 Stage I – Mandatory Submission Requirements**

Stage I will consist of a review to determine which proposals comply with all of the mandatory submission requirements. If a proposal fails to satisfy all of the mandatory submission requirements, the Government will issue the proponent a rectification notice identifying the deficiencies and providing the proponent an opportunity to rectify the deficiencies. If the proponent fails to satisfy the mandatory submission requirements within the Rectification Period, its proposal will be rejected. The Rectification Period will begin to run from the date and time that the Government issues a rectification notice to the proponent. The mandatory submission requirements are set out in Section C of the RFP Particulars (Appendix D).

### **2.3 Stage II – Evaluation**

Stage II will consist of the following two sub-stages:

#### **2.3.1 Mandatory Technical Requirements**

The Government will review the proposals to determine whether the mandatory technical requirements, as set out in Section D of the RFP Particulars (Appendix D), have been met. Questions or queries on the part of the Government as to whether a proposal has met the mandatory technical requirements will be subject to the verification and clarification process set out in Part 3.

#### **2.3.2 Rated Criteria**

The Government will evaluate each qualified proposal on the basis of the non-price rated criteria as set out in Section F of the RFP Particulars (Appendix D).

### **2.4 Stage III – Pricing**

Stage III will consist of a scoring of the submitted pricing of each qualified proposal in accordance with the price evaluation method set out in Pricing (Appendix C). The evaluation of the price will be undertaken after the evaluation of mandatory requirements, and rated criteria has been completed.

### **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 direct contract negotiations to finalize the agreement with the Government. In the event of a tie, the selected proponent will be the proponent selected by way of the lowest price.

## **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 (Part 3) and will not constitute a legally binding offer to enter into a contract on the part of the Government or the proponent and there will be no legally binding relationship created with any proponent prior to the execution of a written agreement. The terms and conditions found in the Form of Agreement (Appendix A) intended to provide the proponent advance notice of some of the key contractual provisions including indemnities, limitation of liabilities, service requirements, etc. that would be contained in the form of contract and are to form the basis for commencing negotiations between the Government and the selected proponent. Negotiations may include requests by the Government 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 the Government for improved pricing or performance terms from the proponent.

## **2.5.3 Time Period for Negotiations**

The Government intends to conclude negotiations and finalize the agreement with the top-ranked proponent during the Contract Negotiation Period, commencing from the date the Government invites the top-ranked proponent to enter negotiations. A proponent invited to enter into direct contract negotiations should therefore be prepared to satisfy the pre-conditions of award listed in Section E of the RFP Particulars (Appendix D), 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 Section E of the RFP Particulars (Appendix D) are not satisfied or if the parties cannot conclude negotiations and finalize the agreement for the Deliverables within the Contract Negotiation Period, the Government 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 the Government 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.

[End of Part 2]

## **PART 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.

#### **3.1.2 Proposals in English**

All proposals must be written in the English language only.

#### **3.1.3 No Incorporation by Reference**

The entire content of the proponent's proposal should be submitted in a fixed form, 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 References and Past Performance**

In the evaluation process, the Government may include information provided by the proponent's referees and may also consider the proponent's past performance or conduct on previous contracts with the Government or other institutions.

#### **3.1.5 Information in RFP Only an Estimate**

The Government and its advisers make no representation, warranty or guarantee as to the accuracy of the information or empirical data 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, travel or demonstrations.

#### **3.1.7 Proposal to be Retained by the Government**

The Government 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**

The Government 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. The Government may contract

with others for goods and services the same as or similar to the Deliverables or may obtain such goods and services internally.

### **3.1.9 Equivalency**

When proprietary names, brands, catalogues or reference numbers are specified in the Deliverables, they are intended to set a minimum standard, and preference for any particular material or equipment is not intended. The proponent may offer material or equipment of similar characteristics, type, quality, appearance, finish, method of construction and performance and if doing so must disclose any difference in the characteristics, type, quality, appearance, finish, method of construction or performance of the material or equipment.

## **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 directed to anyone other than the RFP Contact. The Government is under no obligation to provide additional information, and the Government 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 from the RFP Contact on any matter it considers to be unclear. The Government is not responsible for any misunderstanding on the part of the proponent concerning this RFP or its process.

### **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 the Government, 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. All addenda will be published online at <https://www.gov.bm/procurement-notices>. 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 the Government. In the Submission Form (Appendix B), proponents must confirm their receipt of all addenda by setting out the number of each addendum in the space provided.

### **3.2.3 Post-Deadline Addenda and Extension of Submission Deadline**

If the Government determines that it is necessary to issue an addendum after the Deadline for Issuing Addenda, the Government may extend the Submission Deadline.

### **3.2.4 Verify, Clarify and Supplement**

When evaluating proposals, the Government may request further information from the proponent or third parties in order to verify, clarify or supplement the information provided in the proponent's proposal. The information may include, without limitation, clarification with respect to whether a proposal meets the mandatory technical requirements set out in Section D of the RFP Particulars (Appendix D). The Government 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 the Agreement is executed by the Government and a proponent, the other proponents may be notified directly in writing 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 sixty (60) days of such notification.

#### **3.3.3 Procurement Protest Procedure**

If a proponent wishes to challenge the RFP process, it should provide written notice to the RFP Contact in accordance with the Government's Complaints and Disputes procedures. The notice must provide a detailed explanation of the proponent's concern with the procurement process or its outcome.

### **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 the Government in the preparation of its proposal that is not available to other proponents, (ii) 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 (iii) 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; or
- (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**

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

### **3.4.3 Disqualification for Prohibited Conduct**

The Government may disqualify a proponent, rescind an invitation to negotiate or terminate a contract subsequently entered into if the Government 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 B).

### **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 shall not in relation to this RFP or the evaluation and selection process, engage directly or indirectly in any form of political action or other activity whatsoever to influence or attempt to influence Parliament, the Government, or to influence or attempt to influence any legislative or regulatory action, in the selection or evaluation of any proponent.

### **3.4.7 Illegal or Unethical Conduct**

The proponent represents, warrants, and covenants that, in connection with activities performed under this Agreement or on behalf of the Government, the proponent has not and will not offer, promise, authorise, pay, or act in furtherance of an offer, promise, authorization, or payment of anything of value, directly or indirectly, to a Government Official (as hereinafter defined), political party or party official, candidate for political office, or official of a public international organisation, in order to obtain or retain business, to secure an improper advantage or benefit of any kind or nature to person(s) related, associated or linked to the Government Official, or to secure or influence discretionary action, inaction or a decision of a Government Official(s). For purposes of this proposal, the term "Government Official" shall mean and include any official, public officer or employee of the Government, as well as an official or employee in the judicial, legislative, or military, anyone acting in an official capacity for the Government, or any immediate family member of such persons. The proponent represents, warrants, and covenants that it has complied and will comply with *The Bribery Act 2016* and all other applicable laws of any relevant jurisdiction in connection with the performance of this Agreement. Without limiting the generality of the foregoing, the proponent represents, warrants, and covenants that it has not and will not take any action that would cause the Government or anyone acting on their behalf to violate or be subjected to penalties under *The Bribery Act 2016*, or the applicable anti-corruption laws of other countries.

The proponent acknowledges and agrees that in the event that the Government believes, in good faith, that the proponent has breached this section, the Government shall have the right to immediately withdraw and terminate this opportunity and terminate any or all other agreements with the proponent.

### **3.4.8 Past Performance or Past Conduct**

The Government may prohibit a supplier from participating in a procurement process based on past performance or based on inappropriate conduct in a prior procurement process, 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; or
- (c) any conduct, situation or circumstance determined by the Government, in its sole and absolute discretion, to have constituted an undisclosed Conflict of Interest.

### **3.4.9 No Collusion**

Proponents must not engage in any collusion and must sign the certificate as set out in the Certificate of Confirmation of Non-Collusion (Appendix E).

## **3.5 Confidential Information**

### **3.5.1 Confidential Information of the Government**

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

- (a) is the sole property of the Government 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 the Government; and
- (d) must be returned by the proponent to the Government immediately upon the request of the Government.

### **3.5.2 Confidential Information of Proponent**

- (a) A proponent should identify any information in its proposal or any accompanying documentation supplied in confidence for which confidentiality is to be maintained by the Government. The confidentiality of such information will be maintained by the Government, except as otherwise required by the Public Access to Information Act 2010 or by order of a court or tribunal.
- (b) Proponents are advised that their proposals will, as necessary, be disclosed, on a confidential basis, to advisers retained by the Government 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.
- (c) The Proponent is responsible to ensure that they comply with the *Personal Information Protection Act 2016* ("PIPA"), related to any information in the proponent's custody, care or control.

### **3.6 Procurement Process Non-Binding**

#### **3.6.1 No Process Contract and No Claims**

This RFP is a request for proposals only and participation in this RFP is not intended to create legal obligations between the Government and any of the proponents or their representatives. For greater certainty and without limitation:

- (a) Participation in this RFP will not give rise to any preliminary contract or collateral contract;
- (b) No proponent shall have any claim for any compensation of any kind whatsoever (whether in contract, tort, law, equity or otherwise), as a result of participating in this RFP, and by submitting a proposal each proponent shall be deemed to have agreed that it has no claim against the Government;
- (c) The decision to award or not to award a contract to any proponent is at the discretion of the Government. The Government shall have no liability to any proponent with respect to the awarding of a contract or the failure to award a contract to any proponent. Proponents acknowledge that the proponent that submits the proposal with the lowest price might not be awarded a contract.

#### **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 the Government 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 the Government to enter into an agreement for the Deliverables.

#### **3.6.4 Cancellation**

The Government may cancel or amend the RFP process without liability at any time. Cancellation may occur, for example, if:

- (a) no qualitatively or financially worthwhile offer has been received or there has been no valid response at all;
- (b) the economic or technical parameters of the project have changed fundamentally;
- (c) exceptional circumstances or force majeure render normal implementation of the project impossible;
- (d) all offers exceed the financial resources available, or are otherwise inconsistent with the principles of economy, efficiency and effectiveness; or
- (e) irregularities require cancellation in the interest of fairness.

The publication of a procurement notice does not commit the Government to implement the programme or project announced.

### **3.7 Governing Law and Interpretation**

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

- (f) are intended to be interpreted broadly and independently (with no particular provision intended to limit the scope of any other provision);
- (g) 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
- (h) are to be governed by and construed in accordance with the laws of Bermuda applicable therein.

[End of Part 3]

## **APPENDIX A - FORM OF AGREEMENT**

The terms and conditions found in the Form of Agreement (Appendix A) are intended to provide advance notice of some of the key contractual provisions of the Agreement, including indemnities, limitation of liabilities, service requirements, etc. that form the basis for commencing Agreement between the Government and the selected proponent.

See Annex A - FORM OF AGREEMENT

## APPENDIX B – SUBMISSION FORM

### 1. Proponent Information

<p>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.</p> <p>If the company is incorporated and registered, then a Certificate of Incorporation and a Certificate of Incumbency is required and must be submitted with the Submission Form.</p> <p><b><u>Declaration of Interest:</u></b> The proponent shall provide details of its ownership and/or managerial structure upon request from the Government. The proponent shall also provide a statement of whether or not it has any relevant and material interest relevant to the provision of the Goods and Services. Such statement shall be provided at least annually or if there is any change in the interest of the proponent.</p>	
Full Legal Name of Proponent or Personal/Given Name:	
Representative Name (Person with Signing Authority) / Title:	
Any Other Relevant Name under which Proponent Carries on Business:	
Street Address:	
City, Province/State:	
Country:	
Postal Code:	
Phone Number:	
Proponent's Social Insurance Number issued by the Government of Bermuda:	
Proponent's Tax Payroll Number issued by the Government of Bermuda:	
Proponent's Registration Number issued by the Bermuda Registrar of Companies (if incorporated):	
Company Website (if any):	
Proponent Contact Name and Title:	
Proponent Contact Phone:	
Proponent Contact Fax:	
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 Process Contract bidding process), and that no legal relationship or obligation regarding the procurement of any good or service will be created between the Government and the proponent unless and until the Government 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 and in Pricing (Appendix C) in particular. 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 requested to confirm that it has received all addenda by listing the addenda numbers, \_\_\_\_\_ to \_\_\_\_\_ (if applicable) issued by the Government, or if no addenda were issued by the Government write the word "None". The onus is on proponents to make any necessary amendments to their proposals based on the addenda. The proponent confirms it has read, received and complied with these addenda. Proponents who fail to complete this section will be deemed to have received all posted addenda.

## **6. No Prohibited Conduct**

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

## **7. Conflict of Interest**

Proponents 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 the Government 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:

---

---

---

---

**8. Disclosure of Information**

Any information collected or used by or on behalf of the Government under this solicitation document is subject to the Public Access to Information Act 2010 (“Act”). The information belongs to a class of information that might be made available to the general public unless it is contained in a record that is exempt from disclosure under the Act. Any questions regarding the collection, use, or disclosure of the information should be directed to the public authority that issued this solicitation document.

---

Signature of Witness

---

Signature of Proponent Representative

---

Name of Witness

---

Name of Proponent Representative

---

Title of Proponent Representative

---

Date

I have the authority to bind the proponent.

**End of Appendix B**

SAMPLE CERTIFICATE OF INCUMBENCY

The undersigned being the Secretary of the company as named below (the "Company"), a company duly organised and existing under the laws of the Islands of Bermuda and having it's registered office as set out below **DO HEREBY CERTIFY** that the following is a true and correct listing of the Directors and Officers of the Company in full force and effect as of the date hereof.

DIRECTORS \_\_\_\_\_

List

ALTERNATE DIRECTORS

List

OFFICERS

List

IN WITNESS WHEREOF I have hereunto set my signature in accordance with the Bye-Laws of the Company.

Company Name: .....

Date: .....

\_\_\_\_\_

Secretary/Director

## APPENDIX C – PRICING

### 1. Instructions on How to Provide Pricing

- (a) Proponents should provide the information requested under section 3 below (“Required Pricing Information”) by reproducing and completing the table below in their proposals, or, if there is no table below, by completing the attached form and including it in their proposals.
- (b) Pricing must be provided in Bermuda funds, inclusive of all applicable duties and taxes, which should be itemized separately.
- (c) Pricing quoted by the proponent 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.

### 2. Evaluation of Pricing

Pricing is worth 25 percent of the total score.

Pricing will be scored based the formula below. Each respondent will receive points of the total possible points allocated to price for the particular category it has bid on, which will be calculated in accordance with the following formula.

2.1 Price (include all cost) (non-construction – goods and services): 5 = lowest bid, 4 = next lowest, etc. until 0 = most expensive

2.2 The respondent is in a stable financial position

Following financial checks, i.e. checking a bank reference, the following scores should be awarded.

5 = all financial checks sound, 3 = minor financial concerns, 1 = major financial concerns, 0 = no evidence provided / evidence of severe financial instability.

2.3 The respondent has no outstanding Government debt

Following financial checks with Social Insurance, the Accountant General's Department's Debt Collection Section, the Bermuda Health Council and the Tax Commissioner, the following scores should be awarded:

5 = all financial checks sound, 3 = minor financial concerns, 1 = major financial concerns, 0 = no evidence provided / evidence of severe financial instability.

In addition to any rectification processes, or rights to verify, clarify and supplement,

- (a) The Government will examine the responses to determine whether they are complete, whether any computational errors have been made, whether the documents have been properly signed, and whether the bids are generally in order.
- (b) Arithmetical errors will be rectified on the following basis:

- (i) Where there is a discrepancy between the unit price and the total price that is obtained by multiplying the unit price and quantity, the unit price shall prevail and the total price shall be corrected. If the Proponent does not accept the correction of errors, its Bid will be rejected. If there is a discrepancy between words and figures the amount in words will prevail;
- (ii) Where there is a discrepancy between the amounts in figures and in words, the amounts in words will govern; and
- (iii) Where there is a discrepancy between the individual lump sums and the total amounts derived for the sum of the individual lump sum, the individual lump sum as quoted will govern, and the total amount will be corrected.

### **3. Required Pricing Information**

See Annex B - Required Pricing Form

## APPENDIX D – RFP PARTICULARS

### A. THE DELIVERABLES

The Information and Digital Technologies department within the Government of Bermuda is seeking a high-maturity Managed Detection and Response (MDR) service provider to provide an integrated, outcome-based security program. The MDR will be required to work alongside the Government of Bermuda who will be the final decision makers on all recommendations.

These services will cover:

1. Strategic Tooling & Outcome Accountability Incident response
2. 24x7 Security Operations Center (SOC) Monitoring & Incident Response
3. Virtual CISO & Security Governance
4. Security Testing – Vulnerability Assessment & Penetration Testing
5. Risk Assessment & Strategic Roadmap
6. Integration with Operations

Unlike a traditional monitoring service, the Information and Digital Technologies department within Government of Bermuda requires a service provider that assumes direct accountability for threat containment and strategic risk reduction. The service provider must align all operations with the National Institute of Standards and Technology (NIST) Cybersecurity Framework, ensuring rigorous compliance with the International Organization for Standardization (ISO) or the International Electrotechnical Commission (IEC) 27001 and Bermuda's Personal Information Protection Act (PIPA). The successful respondent will demonstrate a commitment to zero-trust principles, proactive threat hunting, and a 'best-value' approach that prioritizes measurable security outcomes over manual administrative tasks.

The service provider should provide their methodology to demonstrate their capability to deliver the following critical services:

#### 1. Strategic Tooling & Outcome Accountability:

IDT prioritizes the achievement of measurable security outcomes over the utilization of specific software brands:

1.1 Leveraging Existing Platforms: IDT has made significant investments in Cortex Extended Detection and Response (XDR), Microsoft Defender, Node Zero, Criminal IP and Fortinet Ecosystem. Proponents are strongly encouraged to leverage these existing platforms to ensure cost-efficiency and rapid operational integration.

1.2 Proponent Accountability: While proponents may propose an alternative technology stack, they must justify the move and identify all associated costs as separate line items in the Financial Proposal.

1.3 Certification of Efficacy: Any proponent electing to leverage the existing platforms must formally certify in their response that these tools are sufficient to meet the 60-minute Mean Time to Contain (MTTC) target

#### 2. 24x7 Security Operations Center (SOC) Monitoring & Incident Response:

Description:

A managed SOC capability providing around-the-clock monitoring of all networks and approximately 5,000 endpoints. Services should include continuous threat detection, alert triage, and proactive threat hunting, either using IDT's existing tools, or with recommended vendor tools, as described in Section A.1 above.

The service provider must be able to rapidly investigate and contain incidents, performing digital forensics and root-cause analysis as needed. The service provider is required to provide regular security status reporting and periodic incident simulation/drills to ensure preparedness.

Purpose:

To provide real-time operational security coverage and minimize the impact of any cyber incidents through fast response.

## 2.1 Strategic Speed of Detection and Containment (The "1-10-60" Rule)

- 2.1.1 Mean Time to Detect (MTTD): 100% of critical security events must be detected and surfaced in the service provider's platform within 1 minute of ingestion.
- 2.1.2 Mean Time to Acknowledge (MTTA): SOC analysts must acknowledge and begin triage of critical alerts within 10 minutes.
- 2.1.3 Mean Time to Contain (MTTC): Confirmed high-severity threats (e.g., active ransomware or unauthorized access) must be contained within 60 minutes of detection.

Note: Containment actions include host isolation via Cortex XDR, account suspension, or blocking of malicious IPs/domains.

## 2.2 Response Quality and Forensics

- 2.2.1 Critical Vulnerability Notification: Notification of "Zero-Day" or critical vulnerabilities (Common Vulnerability Scoring System (CVSS) 9.0+) within 24 hours of public disclosure.
- 2.2.2 Root Cause Analysis (RCA): Delivery of a formal RCA and remediation roadmap within 48 hours of incident containment.
- 2.2.3 False Positive Rate: Maintain a false positive rate of less than 10%.

## 2.3 Proactive Readiness

- 2.3.1 Proactive Threat Hunting: Completion of one deep-dive threat hunt per month based on global trends relevant to Bermuda's infrastructure.
- 2.3.2 Incident Simulation: Execution of two annual tabletop exercises to validate that escalation and containment workflows between the service provider and IDT are functional.

## 3. Virtual CISO & Security Governance:

Description:

Providing strategic security leadership and oversight by helping to develop and update security policies, procedures, and standards; guiding risk management processes; and ensuring security is embedded in organizational governance. The vCISO will advise on security investments and architecture, ensuring alignment with the NIST Cybersecurity Framework and other best practices. This includes mapping the Government's security controls to compliance requirements (e.g. PIPA privacy law, Public Access to Information Act, and relevant regulations), defining clear

roles and responsibilities for cybersecurity oversight, and helping train officers on security awareness.

Purpose:

To strengthen strategic cybersecurity posture and ensure continuous governance and compliance.

### 3.1 Policy & Strategic Velocity

- 3.1.1 Strategic Roadmap Delivery: Completion and executive approval of an updated 3-year Cybersecurity Strategic Roadmap within the first 90 days of the contract.
- 3.1.2 Policy Review Cycle: The MDR should review and propose updates for all of core security policies (e.g., Acceptable Use, Incident Response, Data Classification) ensuring alignment with NIST Cybersecurity Framework (CSF) and PIPA annually. The proposals should be sent to IDT management in writing for review.
- 3.1.3 Investment Alignment: Delivery of a Security Investment Analysis report bi-annually, mapping proposed spend to specific risk reductions identified in the NIST framework.

### 3.2 Risk & Compliance Management

- 3.2.1 Risk Register Accuracy: Maintain a live Enterprise Security Risk Register with 100% of "High" and "Critical" risks having documented mitigation plans or formal management sign-off.
- 3.2.2 Compliance Mapping: Completion of a full PIPA and Public Access to Information Act control mapping within 120 days of contract commencement.
- 3.2.3 Audit Readiness: Successful facilitation of at least one internal security audit per year with zero "Critical" findings related to governance or policy gaps.

### 3.3 Governance & Awareness

- 3.3.1 Executive Engagement: Delivery of quarterly executive security briefings to the CIO and relevant Government officers, including a "Maturity Scorecard" based on NIST CSF.
- 3.3.2 Security Awareness Impact: Achievement of a 90% or higher completion rate for annual security awareness training across all 5,000 endpoints/users.
- 3.3.3 Phishing Simulation Resilience: Reduction of the organization's "Phish-Prone %" to below 5% through regular vCISO-led simulation and training.

## 4. Security Testing – Vulnerability Assessment & Penetration Testing:

Description:

Regular security testing services are required to validate and improve the Government's defenses. The service provider should conduct periodic vulnerability assessments across networks, systems, and applications to identify weaknesses, misconfigurations, or compliance gaps. In addition, penetration testing engagements (e.g. annual or bi-annual) simulating real-world attacks to probe critical systems (external and internal) for exploitable vulnerabilities are expected. Emphasis is on thorough testing and timely remediation guidance for any findings. Full-scale red-team exercises are optional; however, service providers may propose red teaming as an added-value service for advanced threat simulation. All testing must be performed in a

controlled manner with minimal disruption, and findings should be documented with clear risk ratings and recommendations.

#### 4.1 Vulnerability Management Efficiency

- 4.1.2 Critical Vulnerability Notification: The service provider must notify the Government of any newly discovered "Critical" vulnerabilities (CVSS 9.0+) within the environment within 24 hours of detection.
- 4.1.3 Vulnerability Triage Accuracy: 100% of detected vulnerabilities must be assigned a risk rating (e.g., CVSS score) and mapped to the specific business impact within 3 business days of a scan.
- 4.1.4 Scanning Coverage: Ensure that 100% of the ~5,000 devices in scope, including cloud-based assets, are successfully scanned for vulnerabilities at least once per month.

#### 4.2 Penetration Testing & Red Teaming Quality

- 4.2.1 Exploitation Success Rate: For annual penetration tests, the service provider must document the specific "attack path" for 100% of successfully exploited vulnerabilities, demonstrating the potential real-world impact.
- 4.2.2 Remediation Validation: Following a penetration test, the service provider must perform a re-test of all "High" and "Critical" findings within 30 days of the Government's reported fix to confirm the vulnerability is closed.
- 4.2.3 Minimal Disruption Compliance: 100% of testing must be performed within the pre-approved maintenance windows, with zero unauthorized service outages caused by testing activities.

#### 4.3 Reporting and Risk Communication

- 4.3.1 Executive Summary Timeliness: A comprehensive report of penetration testing findings, including clear risk ratings and remediation recommendations, must be delivered within 10 business days of the exercise completion.
- 4.3.2 Remediation Velocity Tracking: The service provider must provide a monthly "Vulnerability Aging Report" showing the average time to remediate critical vs. low-risk findings against industry benchmarks.

### 5. Risk Assessment & Strategic Roadmap:

#### Description:

The service provider should build upon recent risk assessment and perform their own in-depth cybersecurity risk assessment to establish a baseline of the Government's security posture. This assessment should include compiling an asset inventory and data classification, analyzing threats and vulnerabilities, and evaluating current security controls against industry standards (such as NIST CSF, ISO 27001, etc). Deliverable from this phase is a strategic roadmap that prioritizes initiatives and investments to address identified gaps and enhance maturity.

All the activities must be continuously monitored and relevant artifacts updated.

#### Purpose:

Inform the ongoing security program (including the SOC, vCISO, and testing activities) and ensure the service provider focuses on the areas of greatest risk.

#### 5.1 Discovery & Inventory Accuracy

- 5.1.1 Asset Inventory Completeness: 100% of network-connected assets (~5,000 devices) must be identified, categorized, and assigned a risk owner within the first 60 days.
- 5.1.2 Data Classification Coverage: Identification and classification of all "Critical" and "Sensitive" data repositories across Government networks, ensuring alignment with Bermuda PIPA. Target is to complete 5 departments per month.
- 5.1.3 Shadow IT Identification: Delivery of a report identifying at least 95% of unauthorized or "Shadow" cloud services currently in use within the infrastructure within the first 60 days.

#### 5.2 Assessment Maturity & Gap Analysis

- 5.2.1 Control Framework Alignment: Completion of a comprehensive gap analysis mapping current security control against 100% of the NIST CSF sub-categories.
- 5.2.2 Threat Modeling Depth: Development of at least five high-impact threat scenarios specific to the Government of Bermuda's infrastructure (e.g., ransomware, data exfiltration) to test control efficacy.
- 5.2.3 Vulnerability Baseline: Establishment of a verified "Technical Debt" baseline, identifying all vulnerabilities older than 180 days that require immediate remediation.

#### 5.3 Strategic Roadmap Execution

- 5.3.1 Roadmap Prioritization: Delivery of a 3-year Strategic Roadmap within 90 days, where 100% of initiatives are prioritized by "Risk Reduction vs. Cost of Implementation".
- 5.3.2 Investment Traceability: 100% of proposed security investments in the roadmap must be mapped to a specific gap identified during the NIST CSF assessment.
- 5.3.3 Maturity Milestone Targets: Definition of target NIST CSF Maturity Scores for years 1, 2, and 3, providing a clear "finish line" for the service provider.

### 6. Integration with Operations:

#### Description:

The service provider will work closely with the Government's internal IT and security personnel. Successful integration will require the service provider to establish communication channels, incident escalation procedures, and possibly on-site coordination for incident response. The proposal should outline how the service provider plans to interface with the Government's IT Service Management processes (e.g. how incidents are ticketed, how changes are approved for remediation actions, etc.). A hybrid delivery model (on-site presence for key activities or reviews, combined with remote 24x7 coverage) is preferred.

#### 6.1 Communication and Escalation Efficiency

- 6.1.1 Escalation Path Accuracy: 100% of critical incidents must be escalated to the correct Government point of contact via the agreed-upon channel (phone/portal) within 5 minutes of triage completion.

- 6.1.2 On-site Response Readiness: For severe incidents requiring on-site coordination, the service provider must have a senior responder available in Bermuda or virtually present via a dedicated "War Room" within 4 hours of request.
- 6.1.3 Communication Channel Uptime: The service provider provided portal and emergency communication lines must maintain 99.9% availability.

## 6.2 IT Security Management (ITSM) & Ticket Integration

- 6.2.1 Ticket Sync Latency: 100% of security incidents must be reflected in the Government's ITSM tool (e.g., ServiceNow) within 10 minutes of creation in the service provider's SOC platform.
- 6.2.2 Bi-directional Status Updates: 100% of status changes or comments made by Government personnel in the ITSM must be visible to the service provider's SOC analysts in real-time.
- 6.2.3 Change Management Compliance: 100% of remediation actions requiring infrastructure changes (e.g., firewall rule updates) must follow the Government's formal Change Advisory Board (CAB) process, with zero unauthorized changes.

## 6.3 Operational Collaboration

- 6.3.1 Meeting Cadence Adherence: 100% completion of weekly operational syncs and monthly service reviews to discuss ticket trends and performance against SLAs.
- 6.3.2 Knowledge Base Contribution: The service provider must contribute at least one documented "Runbook" or SOP update per quarter to the Government's internal knowledge base based on observed incident patterns.

## **B. MATERIAL DISCLOSURES**

### 1. Confidentiality and Non-Disclosure Agreement (NDA)

The successful respondent will be required to ensure that all personnel involved in the execution of the project sign a Non-Disclosure Agreement (NDA) prior to commencing any work. This is to safeguard the confidentiality of sensitive information and ensure that all proprietary, operational, and security-related data of the Bermuda Government is protected. The NDA must be executed by all project staff, including subcontractors or third-party personnel, as a mandatory condition before any access to Bermuda Government systems, data, or facilities is granted. Failure to comply with this requirement will result in delays or suspension of the project until all NDAs are properly executed and submitted.

### 2. Security Vetting

All employees assigned to the contract(s), including subcontractors or third-party personnel, by the successful respondent will be subject to an internal vetting process conducted by the Bermuda Police Service (BPS).

### 3. Acceptance of Deliverables

All deliverables are subject to written approval by the Government of Bermuda and at their sole discretion, reserves the right to request for re-work, deem the deliverables not acceptable.

#### 4. Limitations on Disclosure

To protect the Government of Bermuda security posture, certain information will not be disclosed during the RFP phase. This includes, but is not limited to:

1. Known vulnerabilities or security gaps
2. Active or historical security incidents with sensitive detail
3. Detailed system configurations or privileged access information

Additional information may be provided to the successful respondent, subject to enhanced confidentiality controls and internal approvals.

#### 5. System Overview

The Government of Bermuda comprises 90 departments whose systems include architecture that includes Windows, Linux, Fortinet, CISCO, ISERIES, Google Platform Services with approximately 5000 endpoints and 3000 users. The platform is hybrid: - on-premises, hybrid and cloud/SaaS. Current security platforms are: Cortex Extended Detection and Response (XDR), Microsoft Defender, Node Zero, Criminal IP and Fortinet Ecosystem. Specific details such as platform quantities, high-level network diagrams, detection & response capabilities, will be shared with the successful respondent under enhanced confidentiality controls.

#### 6. Operational Expectations

Service Level Agreements (SLAs) and Key Performance Indicators (KPIs)

##### 6.1 Service Desk

Severity Level	Response Timeline	Update Timeline	80% Resolution of Problems
Priority 1	15 Min	1-2 hrs.	Within 4 business hours
Priority 2	1 hr.	2-4 hrs.	Within 8 business hours
Priority 3	4-8hrs	8-24 hrs.	Within 2 business days
Priority 4	8-12 hrs.	1-2 days	Within 5 business days

##### 6.2 Event Monitoring

Service Levels	Response Time/Interval
Health check for sensors	every 60 seconds
Health check of sensor data	Every 60 minutes
Service degradation incident escalation	Within 10 min
Customer notification of incident	Within 10 min
Incident assessment by engineer	within 4 hours

##### 6.3 Event Reaction & Resolution

Service Level	Response Time
---------------	---------------

Mean Time to Detect (MTTD)	<100 minutes
Alarm Time to Triage (TTT)	<30 minutes
Alarm Time to Qualify (TTQ)	< 4 hrs.
Mean Time to Acknowledge (MTTA)	<15 minutes
Mean Time to Investigate (MTTI)	<30 minutes
Mean Time to Resolve (MTTR)	variable 4-24 hrs
Mean Time to Contain (MTTC)	<5 hrs.
Mean Time to Recover (MTTR)	<30 minutes

### **C. MANDATORY SUBMISSION REQUIREMENTS**

#### **1. Submission Form (Appendix B)**

Each proposal must include a Submission Form (Appendix B) completed and signed by an authorized representative of the proponent.

#### **2. Pricing (Appendix C)**

Each proposal must include pricing information that complies with the instructions contained in Pricing (Appendix C).

#### **3. Certificate of Confirmation of Non-Collusion (Appendix E)**

Each proposal must include a Certificate of Confirmation of Non-Collusion Form (Appendix E) completed and signed by an authorized representative of the Proponent.

#### **4. Company Certificate of Incorporation**

A signed copy of the Certificate of Incorporation must be included for proponents that are companies/corporations.

#### **5. Other Mandatory Submission Requirements**

##### **5.1 Company Profile**

Respondents must provide a brief overview of the company, including years in business, organizational structure, and relevant experience in providing comprehensive cyber security services.

See Annex C - Company Profile Form

##### **5.2 Local Benefits**

The respondents must complete and submit a completed Local Benefits form.

See Annex D - Local Benefits.

##### **5.3 Certifications**

Respondents must provide valid ISO/IEC, NIST, SOC2/IS0 27001 or any other relevant certifications as of the submission deadline of this RFP. The contractor will be required to maintain these certifications over the term of the Contract.

#### **5.4 Letter of good financial standing**

Respondents must provide a letter of good financial standing issued within the last six (6) months from a recognized financial institution confirming the company's financial stability and a signed declaration of financial solvency and ability to meet contractual obligations.

#### **5.5 Technical Proposal - Proposal Submission Requirements**

To achieve a uniform review process and obtain the maximum degree of comparability, it is required that the proposals be organized in the manner specified below. Proposals shall not exceed forty(40) pages in length (excluding letter of transmittal, resumes, title page(s), and index/table of contents, attachments or dividers). Information in excess of those allowed will not be evaluated/scored. No links will be acceptable.

One page shall be interpreted as one side of single lined, typed, 8 1/2" X 11", piece of paper.

##### **5.5.1 Title Page**

Show the RFP number and subject, the name of your firm, address, telephone number(s), name of a contact person, and date.

##### **5.5.2 Table of Contents**

Clearly identify the materials by section and page number.

##### **5.5.3 Letter of Transmittal (Limited to two (2) pages).**

5.5.3.1 Briefly state an overview of your firm and the firm's understanding of the services to be performed and make a positive commitment to provide the services as specified. State your approach to the project with a timeline and deliverables.

5.5.3.2. Give the name(s) of the person(s) who are authorized to make representations for your firm, their titles, address, and telephone numbers.

5.5.3.3. The letter must be signed by a corporate officer or other individuals who have the authority to bind the firm.

##### **5.5.4. Experience**

5.5.4.1. Detail the firm's experience in the same or similar areas of expertise, stability, and its adaptability to providing the required services.

5.5.4.2. Provide at least three (3) examples of projects completed that are similar in size and nature within the last 3 years. These projects should include the scope and outcomes and must have been completed by current members of your staff. Include a point of contact, telephone number, and a brief description of the services provided.

#### 5.5.5. Primary Account Representative's

Provide detailed information on the qualifications and experience of the Primary Account Representatives as it relates to the required services. Provide details of each representative's background, education, experience and an average number of accounts of the representative are to be assigned to the account.

#### 5.5.6. Key Project Staff

Identify key project staff expected to provide services on behalf of the firm. This should include all service provider third-party personnel and subcontractors. Resumes should be included for each of the individuals referenced.

#### 5.5.7. Available Resources

Provide information on resources available to your firm which indicates that you have access to the services necessary to perform the work.

#### 5.5.8. Contractor Location

Describe the firm's location where the primary services are to be provided and the ability to meet in person with Department personnel when required during the performance of the contract. (Vendors residing and delivering primary services within Bermuda will be eligible for local Benefit points).

#### 5.5.9. Project Methodology and Approach

Provide detailed information on the service provider methodology in meeting the scope of work requirements identified in Appendix D. Describe the overall approach to include any special considerations which may be unique to Government and Bermuda's environment.

### **D. MANDATORY TECHNICAL REQUIREMENTS**

#### **1. Project Team Qualifications**

Respondents must have at a minimum the following certifications or equivalent:

##### 1.1. The Company:

###### 1.1.1. Service Organization Control 2 (SOC2)

###### 1.1.2. Internal Organization for Standardization (ISO) 27001

##### 1.2. Staff

At least one person:

###### 1.2.1. Must be a Certified Information Systems Security Professional (CISSP).

###### 1.2.2. Must have a minimum of 3 years' experience within cybersecurity.

These certifications should be valid and maintained throughout the course of the contract.

## E. PRE-CONDITIONS OF AWARD

### Financial Checks

Prior to awarding a contract to the selected proponent, the contracting department will perform financial checks to confirm whether the proponent is delinquent in making payments to the Government for Social Insurance contributions, Payroll Tax or any other debt recorded by the Accountant General's Debt Collection Section, and will perform a check with the Bermuda Registrar of Companies to confirm whether the proponent is a proper legal entity that is in good standing.

## F. RATED CRITERIA

The following sets out the categories, weightings and descriptions of the rated criteria of the RFP. Proponents who do not meet a minimum threshold score for a category will not proceed to the next stage of the evaluation process.

#	Category	Weighting (%)	Threshold
1	Pricing	25	N/A
2	Experience and Technical Capacity	45	25
3	Local Benefits	30	N/A
<b>Total Points</b>		100	

### 1. Experience and Technical Capacity

Each proponent should provide the following in its proposal:

- 1.1 a brief description of the proponent;
- 1.2 a description of its knowledge, skills, and experience relevant to the Deliverables; and
- 1.3 the roles and responsibilities of the proponent and any of its agents, employees, and subcontractors who will be involved in providing the Deliverables, together with the identity of those who will be performing those roles and their relevant respective expertise.

The following questions will be considered when each proposal is evaluated: -

- 1.4 Does the proponent clearly demonstrate the ability to meet the Government's requirements?
- 1.5 Has the proponent demonstrated experience as an MDR service provider to public sector clients?
- 1.6 Does the proponent offer evidence that they can provide 24x7 SOC Monitoring & Incident Response using the 1-10-60 rule?
- 1.7 Does the proponent offer evidence that they can fulfil the Virtual CISO & Security Governance responsibilities by providing a 3-year road-map?
- 1.8 Does the proponent offer evidence that they can perform the required Security Testing?
- 1.9 Does the proponent provide a Risk Assessment & Strategic Roadmap?
- 1.10 Does the proponent offer evidence that they can integrate with Operations?
- 1.11 Can the proponent lead, facilitate, and coordinate project planning and execution?
- 1.12 Has the proponent performed well on previous Government Projects?
- 1.13 Is the proponent able to complete the work within the required timeframe?
- 1.14 Does the proponent offer evidence that they have sufficient, suitably experienced resources available to complete the work?

## **2. Financial Analysis**

See Appendix C – Pricing

## **3. Local Benefits**

The Government has established the minimum evaluation weight regarding Local Benefits for this procurement at 30% of the total points.

The local benefit considerations will be given to each of the following factors when proposals are evaluated:

### Local Workforce Utilization

- 3.1 Engagement of Bermudian employee (%) during the project.
- 3.2 Number of Bermudians employed by the proponent.
- 3.3 Is the proponent a local specified business? (See the Code of Practice for Project Management and Procurement on the Government's Portal for the definition of "Specified Business")
- 3.4 Use of local specified businesses in the proponent's supply chain.
- 3.5 Use of local specified business as subcontractors (if applicable).
- 3.6 Does the proponent offer evidence of (i) providing mentoring, apprenticeships or training opportunities for Bermudians, or (ii) being willing to offer them?
- 3.7 Does the proponent have (i) a safety and health policy; (ii) a sustainable goods and/or services policy; (iii) and an environmental policy?

See Annex C - Local Benefits

## APPENDIX E – CERTIFICATE OF CONFIRMATION OF NON-COLLUSION

### Notes for the proponents

The essence of Open Tendering is that the Government of Bermuda shall receive bona fide competitive proposals from suitably qualified persons or entities. In recognition of this principle, each person or entity that submits a proposal will be required, by way of the signature of a duly authorized representative of the company, to confirm that the proposal has been submitted without any form of collusion.

All proponents must complete and sign a Certificate of Confirmation of Non-Collusion. Any proposals submitted which do not include a signed copy of the Certificate will be wholly rejected and will not be included in the evaluation process.

If it is later found that the undertakings made below have been breached at any stage of the procurement process, then the proponent will be expelled from the process immediately. In the event that this is discovered after a contract award, legal action may be taken against the proponent and/or any party involved in the matter.

Any proponent that submits false information in response to this Request for Proposals (RFP), and any other person or entity involved in collusion, may be excluded from competing for future contracts tendered by the Government of Bermuda.

### Confirmation of non-collusion

I/We certify that this is a bona fide proposal, intended to be competitive and that I/We have abided by the terms and conditions related to this proposal and that I/We have not fixed or adjusted the amount of the proposal or the rates and prices quoted by or under or in accordance with any agreement or arrangement with any other person.

I/We confirm that we have not received any information, other than that contained within the RFP pack, or supplementary information provided to all proponents.

I/We also certify that I/We have not done and undertake that I/We will not do at any time any of the following acts:

- (a) communicating to a person other than the RFP Contact the amount or approximate amount of my/our proposed proposal (other than in confidence in order to obtain quotations necessary for the preparation of the proposal for insurance);
- (b) entering into any agreement or arrangement with any other person that he shall refrain from competing or as to the amount of any proposal to be submitted; or
- (c) offering or agreeing to pay or give or paying any sum of money, inducement, gift /hospitality or valuable consideration directly or indirectly to any person in relation to this procurement.

By signing this document, I/we have read and agree to its terms and conditions.

(1) \_\_\_\_\_ Title \_\_\_\_\_ Date \_\_\_\_\_

(2) \_\_\_\_\_ Title \_\_\_\_\_ Date \_\_\_\_\_

for and on behalf of \_\_\_\_\_