Coimisiún na Meán

REQUEST FOR TENDERS

Open Procedure

Request for Tender for the Provision of Chief Information Security Officer (CISO) as a Service and Associated Cyber Security Advisory and Specialist Support Services

Deadline for receipt of Tenders:	**4th August 2026 at 15:00**
Deadline for queries:	**24th July 2026 at 15:00**
All queries must be submitted via the eTenders messaging function.	
Responses to clarifications will be posted on www.etenders.gov.ie	
Tenders must be submitted via www.etenders.gov.ie only.	

Table of Contents

1. INTRODUCTION

1.1 Information about Coimisiún na Meán

The Online Safety and Media Regulation Act ("OSMR Act") 2022 was commenced on 15 March 2023, on which date the Broadcasting Authority of Ireland (BAI) was dissolved and **Coimisiún na Meán** ("the Commission"), a new independent regulator, was established.

In addition to assuming the functions previously exercised by the BAI in its role as independent regulator for radio and television broadcasting services in Ireland, the OSMR Act provides for the transposition of the revised Audiovisual Media Services Directive (AVMSD), an updated regulatory framework for broadcasting services and on-demand audiovisual media services, and the establishment of a new regulatory framework for online safety.

As an independent regulator, the Commission will oversee and enforce these new and updated regulatory frameworks **and will play** a key role in the development and funding of the wider media sector. Coimisiún na Meán will devise and implement a Media Fund, in line with the recommendations of the Future of Media Commission, with a range of schemes to support public service content and digitalisation in the sector. It will advise the Minister on the creation of a European Works Levy to fund new audiovisual works in line with the provisions of the OSMR Act.

The Commission will also play a key role in stimulating greater equality, diversity and inclusion in the media and in supporting sustainability through environmental initiatives across the wider media sector. In cooperation with other bodies, the Commission will have a strong role in supporting the Irish language in media services and in promoting educational and training initiatives, in particular in relation to online safety and media literacy.

Given the significantly expanded regulatory framework for the regulation of media and online services set out in the OSMR Act, Coimisiún na Meán has been established as a multi-person Commission, led initially by three Commissioners — an Online Safety Commissioner, a Media Development Commissioner and a Broadcasting Commissioner — together with an Executive Chairperson.

2. SCOPE OF CONTRACT

The Commission is seeking the provision of Chief Information Security Officer (CISO) Advisory Service and associated cyber security advisory and specialist support services.

The Services will comprise two primary components:

Part 1 – CISO Advisory Service and ICT Cyber Security Services

The first component of the Services relates to the provision of CISO Advisory Service and ICT-focused cyber security advisory support to An Coimisiún's ICT team. This will include the provision of expert guidance, advice and support in respect of information security governance, cyber security risk management, ICT policies, procedures, processes and technical controls.

The successful Tenderer will be required to support An Coimisiún in ensuring that its ICT environment, information security arrangements and cyber security practices are aligned with applicable public sector requirements, recognised industry best practice and relevant standards, including ISO/IEC 27001.

Part 2 – Non-ICT Cyber Security Support Services

The second component of the Services relates to the provision of specialist cyber security advisory and support services to business units across An Coimisiún outside of core ICT operational activities. These Services are intended to support An Coimisiún in meeting broader statutory, regulatory and operational obligations arising across its functions and regulatory remit.

The Contract shall commence on the date of contract execution and shall continue for an initial period of three (3) years. The Commission reserves the right, at its sole discretion, to extend the Contract for up to two (2) further periods of twelve (12) months each, subject to satisfactory performance, continued business requirements and the availability of funding.

The maximum possible duration of the Contract shall therefore be five (5) years.

This procurement is being conducted using the Open Procedure in accordance with applicable public procurement law.

The Commission reserves the right to undertake related or similar activities outside the scope of this Contract, including through other contractual arrangements.

The deadline for receipt of Tenders is 4th August 2026 at 15:00.

3. BUDGET, PAYMENT AND COSTS

The estimated maximum value of the Contract is €500,000 excluding VAT over the maximum possible five-year term.

The Commission anticipates that expenditure under the Contract will comprise:

- a retained CISO Advisory Service and associated cyber security advisory support services (Part 1), for which annual expenditure is not to exceed €50,000 excluding VAT; and

- optional specialist cyber security support services (Part 2), which may be procured on a drawdown basis as required. Annual expenditure on such services is not expected to exceed €50,000 excluding VAT.

The figures set out above are estimates only and are provided for indicative purposes. They do not constitute a commitment, guarantee or forecast of expenditure by the Commission.

The actual value of Services procured under the Contract will depend on operational requirements, business needs, available funding and the Commission's demand for Services during the Contract term.

No guarantee is given in relation to the volume, frequency or value of Services to be procured under the Contract.

The Commission shall not be responsible for any errors in the calculation of costs provided in response to this Request for Tenders. Tenderers are responsible for ensuring that all pricing submitted is accurate, complete and inclusive of all costs associated with the delivery of the Services.

Payment will be made on the basis of valid invoices submitted in accordance with the Commission’s payment terms, as set out in Appendix 2 – Terms and Conditions of Supply of Services.

Tenderers shall submit all pricing using the Pricing Schedule provided as a separate document. The Pricing Schedule forms part of the Tender and must be completed and submitted in full.

All costs shall be provided in Euros (€) and shall be exclusive of Value Added Tax

4. INSTRUCTIONS TO TENDERERS

4.1 Tender Documents - Ambiguity, Discrepancy, Error, Omission

If a Tenderer considers that it is missing any document or information which would prevent the submission of a comprehensive Tender, the Tenderer should notify the Commission via the eTenders messaging function as soon as possible.

Tenderers shall immediately notify the Commission if they become aware of any ambiguity, discrepancy, error or omission in the Request for Tenders. Upon receipt of such notification, the Commission shall issue a written clarification or ruling, which shall be communicated to all Tenderers via eTenders and shall form part of the Request for Tenders.

4.2 Deadline for receipt of tenders

The deadline for receipt of Tenders is **4th August at 15:00.**

4.3 Queries

All queries relating to this competition must be submitted via the **eTenders messaging function**.

Clarifications and responses will be issued through eTenders and will be made available to all Tenderers to ensure equal treatment.

Deadline for queries: 24th July 2026 at 15:00

4.4 Submission of tenders

Tenders must be submitted electronically via www.etenders.gov.ie.

Tenders submitted by any other means, including hard copy, email or fax, will not be considered. Late Tenders will not be accepted.

4.4.1 Format for submission of tenders

Tender submissions must be completed using the **Tender Response Document and the accompanying pricing schedule.**

Tenderers should note that page limits apply to certain qualitative award criteria, as specified in the Tender Response Document.

The format of the Tender Response Document must be complied with, and each requirement must be responded to in the order set out in the document.

The Tender Response Document is provided in Word format to allow additional pages or text boxes to be inserted where necessary. Tenderers must **not** submit responses to award criteria in separate appendices or standalone documents.

Tenderers must submit a completed Pricing Schedule as a separate document. Pricing information must not be included within responses to qualitative award criteria unless expressly requested.

4.4.2 European Single Procurement Document (eESPD)

As this procurement exceeds the applicable EU threshold, Tenderers are required to complete and submit the European Single Procurement Document ("eESPD") as part of their Tender submission.

The eESPD constitutes a self-declaration by the Tenderer that:

- the Tenderer is not subject to any of the exclusion grounds;
- the Tenderer satisfies the Selection Criteria set out in this Request for Tenders; and
- the Tenderer will, upon request and without delay, provide the supporting documentary evidence required by the Commission.

Where a Tender is submitted by a consortium, joint venture or group of economic operators, a separate eESPD must be completed and submitted by each participating entity.

Where a Tenderer relies on the capacity of another entity, including a subcontractor, to satisfy Selection Criteria, a separate eESPD must also be submitted for each such entity.

Failure to provide a completed eESPD where required may result in the Tender being deemed non-compliant and excluded from further consideration.

4.5 Qualification of tenders

Qualifications, conditions or caveats attached to a Tender may be regarded as a counteroffer and may result in the Tender being deemed non-compliant and rejected.

4.6 Modifications to tenders prior to the closing date for receipt of tenders

Tenderers may modify or withdraw their Tender at any time prior to the deadline for receipt of Tenders by submitting a revised Tender via eTenders.

The most recent valid submission received via eTenders by the deadline will be deemed to be the Tenderer's final Tender. No modifications will be accepted after the deadline.

4.7 Extension of tender period

The Commission reserves the right, at its sole discretion, to extend the deadline for receipt of Tenders by issuing a notice to Tenderers via eTenders prior to the original closing date.

4.8 Cost of preparation of tender

The Commission will not be liable for any costs incurred by Tenderers in the preparation or submission of Tenders or in relation to any associated activities.
Tenderers are responsible for ensuring that they fully understand the requirements of this Request for Tenders and for any costs incurred in attending clarification or other meetings, where required.

4.9 Tender Validity Period

Tenders shall remain valid for a period of **six (6) months** from the deadline for receipt of Tenders.

4.10 Currency

Tender prices may be submitted in Euro only. All invoices and payments will be in Euro only.

4.11 Confidentiality

This Request for Tenders is issued solely for the purpose of obtaining Tenders for the Services described herein and does not confer any right to use the documentation for any other purpose.

Tenderers shall treat all information supplied in connection with this competition as confidential and shall not disclose such information to any third party except where necessary for the preparation of a Tender.

Given the nature of the Services, Tenderers are expected to maintain appropriate standards of information security and confidentiality in relation to all information accessed, processed or received in connection with this competition.

The Commission will use reasonable endeavours to treat confidential information received from Tenderers as confidential, subject to its obligations under applicable law, including the Freedom of Information Act 2014.

4.12 Conflict of interest

Tenderers must disclose any actual, potential or perceived conflict of interest which may arise in relation to this procurement competition or the delivery of the Services.
This includes, but is not limited to:

- relationships with regulated entities;
- relationships with technology providers, platforms or service providers relevant to the statutory functions of the Commission;

- prior or existing engagements which could impair independence or objectivity; and
- any registerable interest involving the Tenderer and the Commission, its employees or related parties.

The terms “registerable interest” and “relative” shall be interpreted in accordance with Section 2 of the Ethics in Public Office Act 1995.

Where a conflict of interest arises after submission of a Tender, the Tenderer must immediately notify the Commission in writing.

Failure to disclose a conflict of interest may result in exclusion from the competition or termination of any resulting Contract, where appropriate.

4.13 Freedom of Information Act

Each of the parties will undertake to use their reasonable endeavours to hold confidential any confidential information received from the other party, subject to The Commission’s obligations under law, including (if applicable) the provisions of the Freedom of Information Act 2014. The tenderer will agree that, should it wish any confidential information supplied by it to The Commission not to be disclosed, because of its commercial sensitivity, it will, when supplying such information, identify same and specify the reasons for its sensitivity. The Commission will consult with the tenderer about such sensitive information before making a decision regarding release of such information under the Freedom of Information Act 2014. However, The Commission will give no undertaking or assurance that such information will not be released under the provisions of the Freedom of Information Act 2014 and the final decision on whether or not to release such information rests with The Commission or as set out in the Freedom of Information Act 2014.

4.14 Data protection

In this clause, “Data Protection Laws” means all applicable national and EU data protection laws, regulations and guidelines including, but not limited to, Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (the “General Data Protection Regulation”) and any guidelines and codes of practice issued by the Office of the Data Protection Commissioner or other supervisory authority for data protection in Ireland from time to time.

The Commission will be a data controller (where Data Controller has the meaning given to it under the Data Protection Laws) in respect of any Personal Data (where Personal Data has the meaning given to it under the Data Protection Laws) required to be provided by the Tenderer in response to this RFT.

The Tenderer, as Data Controller in respect of any data provided by it in its Tender, is required to confirm in the statement required in the Form of Tender in Tender Response Document that all Data Subjects (where Data Subject has the meaning given to it under the Data Protection Laws) whose Personal Data is provided by the Tenderer have consented to the processing of such Personal Data by the Tenderer, The Commission and the assessment panel for the purposes of the participation of the Tenderer in this Competition or that the Tenderer has a legal basis for providing such Personal Data to The Commission for the purposes of its participation in this Competition.

Note to tenderers: If providing personal data, please provide ALL personal data in a separate appendix to the main body of your tender submission.

4.15 Tax Clearance Certificate

It will be a condition for the award of contract that the tenderer can demonstrate tax clearance throughout the lifetime of the contract. See Irish Revenue web site www.revenue.ie.

4.16 Irish Legislation

Tenderers should be aware that Irish national legislation applies in matters such as employment, working hours, official secrets, data protection, and health and safety. All relevant aspects of such legislation must be observed at all times by the successful service providers.

Tenderers must also have regard to statutory terms relating to minimum pay and to legally binding industrial or sectoral agreements in preparing tenders and delivering services under a contract.

4.17 Determination of responsiveness

After the official opening of tenders, The Commission or its staff or agents will determine whether each tender is substantially responsive to the requirements of this Request for Tenders.

If a material deviation exists that limits in any substantial way The Commission's rights or the tenderer's obligations under the contract, the tender shall be rejected.

4.18 Clarification of tenders

Without prejudice to the conduct of the open procedure, to assist in the examination and comparison of tenders, The Commission may ask tenderers for clarification of aspects of their tenders, including a breakdown of the financial proposal or other information.

4.19 Consortia and Prime/Subcontractors

Where a group of undertakings submit a tender in response to this RFT, The Commission will deal with all matters relating to this public procurement competition through the entity who will carry overall responsibility for the performance of the contract only ("Prime Contractor"), irrespective of whether or not tasks are to be performed by a subcontractor and/or consortium members.

4.20 Correction of errors

The Commission may examine Tenders for arithmetical errors. Where there is a discrepancy between figures and words, the amount in words shall prevail. Where there is a discrepancy between a unit rate and an extended total, the unit rate shall prevail unless the Commission determines that a manifest error has been made. Any correction will be notified to the Tenderer for confirmation. Where a Tenderer does not accept the correction, the Commission may reject the Tender.

4.21 Abnormally Low Tenders

Where a Tender appears to the Commission to be abnormally low in relation to the Services, the Commission reserves the right to request written clarification from the Tenderer regarding the price or costs proposed.

Such clarification may include, but is not limited to, information relating to the economics of the method of delivery, the technical solution proposed, the Tenderer's assumptions, compliance with applicable environmental, social and labour law obligations, and any other matter relevant to the price or costs proposed.

The Commission reserves the right to reject a Tender where the Tenderer fails to provide a satisfactory explanation for the price or costs proposed.

4.22 Interference

Any effort by the tenderer to unduly influence The Commission, relevant The Commission personnel or any other relevant persons or bodies in the process of examination, clarification, evaluation and comparison of tenders and in decisions concerning the award of contract shall have their tender rejected. In accordance with Section 38 of the Ethics in Public Office Act 1995 any money, gift or other consideration from a person holding or seeking to obtain a contract will be deemed to have been paid or given corruptly unless the contrary is proved.

4.23 Inducements to purchase

The Commission shall be entitled to disqualify a tenderer in the following circumstances:

- If the tenderer has offered or given or agreed to give to any person any gift or consideration of any kind as an inducement or reward for doing or forbearing to do, or for having done or forborne to do, any action in relation to the obtaining or execution of this contract award procedure or showing or forbearing to show favour or disfavour to any person in relation to this contract award procedure or any other contract award procedure with The Commission, or

- If like acts have been done by any other person employed by the tenderer or acting on its behalf (whether with or without the knowledge of the tenderer).

The Competition Act, 2014 makes it a criminal offence for tenderers to collude on prices or terms in a public tender procedure. Where The Commission has reasonable grounds to believe that a tenderer may have been involved in collusion, it shall be entitled to exclude such tenderer from the competition at its sole discretion.

4.24 "Or Equivalent"

Please note in relation to this tender document; where reference is made to a particular make, source, process, trademark, type or patent that this is not to be regarded as a de facto requirement. In all such cases it should be understood that the reference in question is accompanied by the words "or equivalent".

4.25 Notification of tender evaluations

All tenderers will be informed of the outcome of their tender following tender evaluation and subsequent clarifications (if any), as well as of any decisions reached regarding the award of this contract.

4.25.1 Standstill Period

Following notification of the award decision, the Commission will observe the applicable standstill period in accordance with the European Communities (Public Authorities' Contracts) (Review Procedures) Regulations 2010 (as amended).

No contract will be concluded until the expiry of the standstill period.

4.26 Award to runner-up

If for any reason it is not possible to conclude the contract with the designated successful tenderer emerging from this competitive process; or if having concluded the contract The Commission considers that the successful tenderer has not met, or cannot meet its obligations; The Commission reserves the right to award the next highest scoring tenderer

the contract on the basis of the same terms at any time during the tender validity period. This shall be without prejudice to the right of the Commission to cancel this competitive process and/or initiate a new contract award procedure at its sole discretion.

4.27 Payment

The Commission operates in accordance with the European Communities (Late Payment in Commercial Transactions) Regulations 2012 as amended.

4.28 Terms and Conditions

The Contract will be based on the applicable Office of Government Procurement ("OGP") Services Contract, as included with or referenced in the Tender Documents.

Tenderers must submit their Tenders on the basis of the OGP contract terms and conditions applicable to this competition. Tenderers may not submit alternative terms and conditions, and any qualification, caveat or proposed amendment to the OGP contract terms may result in the Tender being deemed non-compliant and rejected.

In the event of any conflict or inconsistency between this Request for Tenders, the Tender Response Document, the Specification of Services and the OGP contract, the order of precedence set out in the OGP contract shall apply, unless otherwise stated in the Tender Documents.

4.29 Law

Both The Commission and the successful tenderer shall comply with Irish law and the jurisdiction of the Irish courts, which will govern the contract.

5. EVALUATION OF TENDERS

5.1 Exclusion Grounds

Tenderers must confirm through the eESPD that none of the mandatory or discretionary exclusion grounds set out under Regulation 57 of the European Union (Award of Public Authority Contracts) Regulations 2016 apply.

The Commission reserves the right to exclude any Tenderer at any stage of the procurement process where:

- a mandatory exclusion ground applies;
- a discretionary exclusion ground applies;
- the Tenderer has provided false or misleading information;
- the Tenderer cannot provide supporting evidence upon request; or

• a conflict of interest or distortion of competition cannot be effectively remedied.

Tenderers will either pass OR fail each of the Selection Criteria in this part 5.1. A tenderer who fails a selection criterion will be excluded from participating in this Competition.

Tenders should use the Tender Response Document to provide the information required under the Selection Criteria.

All self-declared information will be verified prior to the award of the contract. In the event that this verification process reveals that misleading or inaccurate information has been provided, your tender will be rejected from further consideration. Moreover, you may be precluded, at the discretion of The Commission, from participating in future competitions.

Following a request from The Commission, you will have five (5) working days to provide the required evidence. If you are not in a position to provide the required evidence within this timeframe your tender will be eliminated from further consideration.

5.1.1 Confirmation of Eligibility

Tenderers are required to provide the following information in the Tender Response Document:

- Contact information for the Tenderer;
- Details of any proposed partnership, consortium or subcontracting arrangements, including the names of all subcontractors and/or consortium members involved in the delivery of the services;
- A description of the role to be fulfilled by each subcontractor and/or consortium member; and
- The name, title, telephone number and email address of the nominated contact authorised to represent the Prime Contractor.

5.1.2 Economic and Financial Standing

Tenderers must declare in the Tender Response Document that they satisfy the economic and financial standing requirements set out below and that they are capable of providing the supporting evidence upon request and without delay.

Insurance	
Requirement	• Employers Liability Insurance (€13 m)

	• Public Liability Insurance (€6.5m) • Professional Indemnity Insurance (€1m)
Evidence	Tenderers must provide evidence (e.g., certificates of insurance including value of cover, renewal date(s)' and name of insurer(s) that you possess the forms and levels of insurance specified or that these insurances can be put in place if you are successful in this competition using the table in the Tender Response Document
Minimum standard	Evidence from insurer in relation to minimum levels of cover required.

Turnover	
Requirement	Tenderers must have a minimum average annual turnover of €2.5 million over the previous three financial years. The Commission reserves the right to accept other appropriate evidence of economic and financial standing where, for a valid reason, the Tenderer is unable to provide the evidence requested.
Evidence	Tenderers must provide appropriate evidence (e.g., auditor's statement or financial accounts) detailing your turnover for each of the three previous financial years in the relevant table in the Tender Response Document OR if you do not have in your possession the evidence required under this eligibility criterion when submitting your tender proposals, you may, in the interim, complete the Form of

	Self-Declaration provided in the Tender Response Document

Tax clearance	
Requirement	Tenderers will be required to produce a tax clearance access number and tax reference number so that The Commission can verify their tax clearance before the contract is awarded and at any time thereafter.
Evidence	Tenderers must provide a tax clearance access number and tax reference number from the Irish Revenue Commissioners using the table provided in the Tender Response Document OR if you do not have in your possession the evidence required under this eligibility criterion when submitting your tender proposals, you may, in the interim, complete the Form of Self-Declaration provided in the Tender Response Document.

5.1.3 Technical and Professional Ability

Previous experience	
Requirement	Tenderers must have successfully completed at least three (3) contracts of a similar nature, scale and complexity within the previous five (5) years. The Commission may, at its discretion, accept contracts currently in delivery where the Tenderer can demonstrate completion of comparable phases or milestones relevant to the Services being procured. The Commission is seeking evidence of experience in the

	provision of cyber security advisory, governance, assurance, CISO Advisory Service, or related specialist cyber security support services delivered to public sector bodies, regulated entities, or similarly complex organisations.
Evidence	Tenderers must provide details of at least three (3) relevant contracts using the template provided in the Tender Response Document. The information provided should include: • client organisation name; • contract scope and description of services delivered; • duration of the contract; • approximate contract value; • description of the Tenderer's role and responsibilities; and • contact details for a referee. The Commission reserves the right to contact referees for verification purposes.

Minimum Technical Capability	
Requirement	Tenderers must demonstrate that they possess the minimum technical capability, organisational capacity and appropriately qualified personnel necessary to deliver the Services. Tenderers must hold valid certification to ISO 27001 or an equivalent independently certified information security management standard. Tenderers must also demonstrate access to appropriately qualified personnel with relevant cyber security

	certifications and experience appropriate to the Services being procured.
Evidence	Tenderers must provide: • evidence of ISO 27001 certification (or equivalent); • details of the proposed service delivery structure; • details of the proposed key personnel and their roles; • curriculum vitae for all proposed key personnel; and • details of relevant professional certifications held by proposed personnel. Examples of relevant certifications may include: • CISSP; • CISM; • CISA; • CRISC; • GIAC certifications; • CEH; or • equivalent recognised cyber security certifications. Where external partners or subcontractors are proposed to support delivery of the Services, Tenderers must provide details of the relevant arrangements and associated technical capabilities.

Resource Availability and Service Continuity	
Requirement	Tenderers must demonstrate that sufficient resources, service continuity arrangements and escalation mechanisms are in place to support the ongoing delivery of the Services throughout the Contract term.
Evidence	Tenderers must provide: • details of the proposed resource allocation model;

	• arrangements for service continuity and resource backfill; • escalation arrangements for major incidents or urgent support requirements; and • confirmation of the ability to attend in-person meetings in Ireland, where required.

Support Hours	
Requirement	Tenderers must confirm their ability to provide support during the required service hours.
Evidence	Tenderers must confirm that regular support services can be provided between 08:00 and 18:00 Monday to Friday, with escalation support available outside these hours for major incidents, outages or cyber security events where required.

5.1.4 Declarations

Tenderers must complete and sign the following declarations in the Tender Response Document:

a. Declaration of Bona Fides
b. Declaration re. Statutory Obligations

5.1.5 Resource allocation

Tenderers must provide details for the individuals nominated to undertake the contract for The Commission. Comprehensive curriculum vitae must be included for each individual identified. CVs demonstrating the nominated consultant's expertise for the role / project must be provided for all key personnel. Tenderers must guarantee that the above staff shall be fully available for delivery of the goods / services identified.

5.1.6 Form of Tender

Tenderers must complete and sign all declarations and forms contained within the Tender Response Document and must complete and submit the Pricing Schedule provided as a separate document.

5.2 Award / assessment criteria

This Contract will be awarded to the Tenderer submitting the most economically advantageous tender ("MEAT"), identified following application of the award criteria and weightings set out below.

In assessing Tenders, the Commission will evaluate the extent to which each Tender demonstrates a clear understanding of the requirements set out in Appendix 1 – Specification of Services, together with the Tenderer's proposed methodology, service delivery model, resources, relevant experience, governance arrangements, pricing structure and approach to environmental, social and sustainability considerations.

The Commission is not bound to accept the most economically advantageous Tender or any Tender received and reserves the right to accept or reject, in whole or in part, any or all Tenders received.

Criterion	%	Minimum score required[1]
Quality, Experience and Expertise of Proposed Resources (Part 1)	30	18
Tenderers should provide details of the qualifications, expertise, certifications, experience and suitability of the proposed key personnel who will be assigned to deliver Part 1 Services. Tenderers should address, where relevant: • qualifications, expertise, certifications and experience of the proposed Technical Liaison and proposed key personnel • relevant experience of the proposed individuals in delivering CISO Advisory Service and ICT-focused cyber security advisory services; • experience of the proposed individuals in information security governance,		

[1] 60% of the maximum achievable score

cyber risk management and security assurance activities; • experience of the proposed individuals supporting ISO/IEC 27001 aligned environments and information security frameworks; • clearly defined roles and responsibilities of each proposed individual; • availability and commitment of the proposed individuals and replacement strategy, to minimize disruption to service continuity where key personnel become unavailable.		
Ultimate Cost to the Contracting Authority for the Contract Tenderers shall complete the Pricing Schedule in full and submit it as a separate document. The evaluated price shall comprise: • Part 1 – Retained CISO Advisory Service: the annual fixed fee proposed by the Tenderer multiplied by five (5) years, representing the maximum potential duration of the Contract; and • Part 2 – Specialist Cyber Security Support Services: the resource rates submitted by the Tenderer applied to the indicative quantities and usage assumptions set out in the Pricing Schedule. The indicative quantities and usage assumptions used for Part 2 are provided solely for the purpose of tender evaluation and facilitating a fair and transparent comparison of Tenders. They do not constitute a commitment, guarantee or forecast of expenditure by the Commission. The Tender achieving the lowest evaluated cost shall receive the maximum marks available for this criterion.	25	n/a

The score for all other Tenders shall be calculated using the following formula: (Lowest Evaluated Cost ÷ Tenderer's Evaluated Cost) × Maximum Marks Available		
Relevant Experience in Supporting Non-ICT Cyber Security Needs (Part 2)	15	9
Tenderers should provide details of the qualifications, expertise and relevant experience of the proposed key personnel who will deliver Part 2 Services. Tenderers should address, where relevant: • Qualifications, certifications and specialist expertise of the proposed personnel relevant to the Services; • experience of the proposed individuals supporting regulatory, supervisory or legislative cyber security requirements; • experience of the proposed individuals conducting technical and organisational cyber security assessments; • experience of the proposed individuals in online safety, platform regulation or digital regulatory environments; • expertise of the proposed individuals in digital forensics, OSINT, investigation-support activities or similar disciplines; • experience of the proposed individuals relating to AI systems, emerging technologies, age assurance technologies or equivalent areas; • experience of the proposed individuals supporting organisations operating within highly regulated environments		
Proposed Approach to Service Delivery and Delivering a Partnership Model	15	9
Tenderers should provide details of their proposed approach to delivering the Services and maintaining an effective partnership model with Coimisiún na Meán throughout the Contract term. • Tenderers should address, where relevant:		

• mobilisation and onboarding arrangements; • governance and reporting arrangements; • management of retained and optional drawdown services; • escalation and incident management arrangements; • quality assurance and service continuity measures; • collaboration with ICT, MSP providers and internal business units; • knowledge transfer and relationship management arrangements; • proactive service improvement and strategic advisory support; and • management of emerging risks, issues and resource constraints.		
Conflict of Interest Tenderers should demonstrate a clear and robust approach to the identification, management and mitigation of actual, potential or perceived conflicts of interest. Responses should include: • details of any existing or potential conflicts relevant to the Services; • organisational separation arrangements between advisory and implementation functions; • governance and escalation procedures relating to conflicts management; • confidentiality and ethical wall arrangements; • ongoing monitoring and disclosure procedures; and • policies and controls supporting independence and impartiality.	7	4
Presentation	5	3

Tenderers who achieve the applicable minimum thresholds under the qualitative award criteria may be invited to attend a Presentation as part of the evaluation process. The Presentation shall consist of a 20-minute presentation followed by a 10-minute question and answer session. The Presentation will take place in person at Coimisiún na Meán's offices on Shelbourne Road, Dublin 4. The Presentation must be delivered by the proposed Technical Liaison / Lead CISO and may be attended by up to two additional key personnel proposed for delivery of the Services. The Presentation will be based on a practical scenario relevant to the Services being procured. The scenario may require Tenderers to explain how they would: • provide CISO Advisory Service support to Coimisiún na Meán; • respond to a significant cyber security incident or emerging cyber security risk; • support regulatory or legislative cyber security requirements; • engage with internal stakeholders, managed service providers and third-party suppliers; and • provide strategic cyber security advice and governance support within a public sector environment. The detailed scenario and supporting instructions will be issued to Tenderers at least one week in advance of the Presentation. The Presentation will be evaluated solely under this criterion and will assess: • the Tenderer's understanding of the scenario presented; • the appropriateness, practicality and effectiveness of the proposed response; • the Tenderer's approach to cyber security governance, risk management and decision-making;		

• the Tenderer's proposed approach to stakeholder engagement, escalation and service delivery; and • the extent to which the proposed solution demonstrates an understanding of Coimisiún na Meán's operating environment and requirements. The Presentation will not be used to re-evaluate the qualifications, certifications, experience or expertise of personnel already assessed under the written award criteria.		
Environmental, Social and Sustainability Considerations		
Tenderers should provide clear and measurable information regarding the sustainability practices and initiatives that will directly support the delivery of the Services under this Contract. Responses should include details of how the Tenderer will minimise environmental impact through the proposed service delivery model, including the use of remote and hybrid delivery approaches, reduction of unnecessary travel, efficient use of technology infrastructure, and sustainable operational practices relevant to cyber security and ICT consultancy services. Tenderers should also outline any broader corporate sustainability initiatives, recognised environmental certifications or standards held, responsible supply chain practices, employee wellbeing and diversity initiatives, and governance measures that support sustainable and ethical service delivery.	3	2
Total	**100%**	-

Tenderers must achieve a minimum score of 60% of the available marks in each qualitative criterion identified above in order to remain under consideration for award. Failure to achieve the minimum score in any qualitative criterion will result in elimination from further evaluation and the Tender will not proceed to cost evaluation.

5.3 Calculation of 'Ultimate Cost'

In order to arrive at an ultimate cost for comparative purposes, The Commission will use the costs provided in the Form of Tender.

The lowest ultimate cost tender which also meets all of the minimum requirements specified in these tender documents will receive the maximum score achievable under this criterion. The scores of the other valid tenders will be calculated by using the following formula:

Number of points = the cost of the lowest valid tender divided by the ultimate cost of the tender in question and multiplied by the maximum score achievable.

The Commission does not bind itself to accept the most economically advantageous tender or any tender, and reserves the right to accept or reject in whole or in part any or all tenders received, and, in particular, to source the requirement with more than one service provider.

5.4 Verification / clarification meetings

Meetings for the purpose of verification or clarification may be carried out with appropriate Tenderers as part of the evaluation process. Such meetings may be required in order to clarify or verify aspects of the written Tender.

Where Tenderers are invited to Presentation stage, the Presentation will be evaluated only under the published Presentation award criterion.

For the avoidance of doubt, clarification meetings and Presentation stage meetings are separate processes. Clarification meetings will not be scored unless expressly identified as part of the Presentation stage.

APPENDIX 1 – SPECIFICATION OF SERVICES

1. Introduction

Background

Coimisiún na Meán (An Coimisiún) is tendering for a support contract for cyber security services. These services will take the form of a CISO Advisory service and other relevant cyber security support services. There will be 2 components to this contract.

The first will be providing standard Cyber Security services to An Coimisiún's ICT team that would be required by any Public Sector Body (PSB). This will include providing guidance in ensuring that ICT policies, processes and systems deployed in An Coimisiún comply with best practice and that An Coimisiún's existing Information Security Framework and are ISO 27001 aligned. An Coimisiún should also be protected from existing, emerging and evolving threats to its environment including any emerging AI threats. This will also include guidance on ensuring that An Coimisiún is aligned with meeting NIS2 or any other mandated requirements.

The second part of the contract will support non-ICT cyber security needs for business units for legislative obligations. This may include working with internal An Coimisiún teams that are tasked with implementing the Online Safety Framework (OSF), Digital Services Act (DSA) or any other relevant legislation.

The retained CISO Advisory Service and associated cyber security advisory support services under Part 1 are not expected to exceed €50,000 excluding VAT per annum.

Specialist cyber security support services under Part 2 will be procured on a drawdown basis as required. Annual expenditure on Part 2 Services is not expected to exceed €50,000 excluding VAT per annum.

These figures are indicative only and are intended to assist Tenderers in understanding the anticipated scale of the requirement. They do not constitute a commitment, guarantee or forecast of expenditure by Coimisiún na Meán.

As this Contract has an initial term of three (3) years with the option to extend for up to two (2) further periods of twelve (12) months each, the maximum potential value of the Contract is €500,000 excluding VAT over the maximum possible five-year term.

2. Description of Current Environment

Tenderers should note the following information regarding the current ICT and cyber security environment within Coimisiún na Meán.

Coimisiún na Meán has a single main office based at 1 Shelbourne Building, Shelbourne Road, Dublin, D04 NP20. In the past 3 years we have increased from around 40 to approaching 300, which may increase further in the coming years. Staff tend to split their working time between office-based and remote working

We have previously had 2 onsite physical servers, and ran a hybrid setup involving physical onsite domain controllers, virtual domain controllers and a cloud-based Entra ID environment. We are currently transitioning away from an "on-premise" architecture, to be fully cloud-based.

Other hardware we use includes Fortinet Switch, Firewall and Wireless Access Points, Apple Iphones and IPads, and Yealink AV and meeting room equipment. Printers are leased through a 3rd party, and are all HP e877 Colour MFDs

We run a predominantly Microsoft based software-suite, including Windows 11, Teams, Sharepoint, M365 products, but we do support a small number of non-microsoft applications (e.g Adobe, HR System Personio, Finance MS Dynamics Business Central and Sage Payroll application). We also operate a Microsoft Dynamics 365–based CRM platform hosted in the cloud, supporting queries, complaints, and interactions with external stakeholders through the Contact Centre

Our Service desk and some technical services are outsourced to a 3rd party ICT Managed Service Provider (MSP), and we use Service Now, Intune and Ninja One for ticketing and device management. They also provide an MDR/SOC/Siem service using MS Sentinel

The information provided is intended to assist Tenderers in understanding the current operating environment only and does not constitute a guarantee, representation or warranty by Coimisiún na Meán regarding existing infrastructure, systems, services or future requirements.

3. Overview of Requirements

It is expected that the successful tenderer will have a close working relationship with An Coimisiún. With this type of partnership model of working in mind, An Coimisiún is interested in not only examples of where a tenderer has delivered these types of services successfully to other customers but how they went above and beyond obligations in meeting a high level of service delivery.

It is expected that in addition to an account manager role, the primary contract for An Coimisiún will be a technical liaison that can deal directly with requests or delegate them to the appropriate resources.

4. Scope of Services

Coimisiún na Meán (An Coimisiún) is tendering for a support contract for cyber security services. These services will take the form of a CISO Advisory service and other relevant cyber security support services. There will be 2 components to this contract.

Part 1 – CISO Advisory Service and ICT Cyber Security Services

The first component of the Services will comprise the provision of cyber security advisory and governance support services to Coimisiún na Meán's ICT team. This will include providing guidance to ensure that ICT policies, processes and systems comply with recognised best practice and that Coimisiún na Meán's Information Security Framework remains aligned with ISO/IEC 27001 and other applicable standards.

The successful Tenderer shall support Coimisiún na Meán in identifying, managing and responding to existing, emerging and evolving cyber security risks, including risks associated

with emerging technologies and artificial intelligence. The Services shall also include support in relation to NIS2 and any other applicable legislative, regulatory or cyber security obligations. Part 1 shall comprise a retained CISO Advisory Service delivered for the fixed annual fee submitted by the successful Tenderer.

Part 1 shall comprise 2 components

- A retained CISO Advisory Service delivered for the fixed annual fee submitted by the successful Tenderer.
- Drawdown services, as specified in Section 15 below

At a minimum, the retained service shall include:

- Weekly meetings;
- Status updates and reporting;
- Quarterly ICT Risk Register reviews;
- Roadmap implementation reviews (including NIS2 and other cyber security initiatives);
- Responses to routine cyber security queries and requests for advice that can reasonably be addressed through email correspondence, scheduled meetings or brief advisory engagements.

Services under Part 1 shall be invoiced monthly in arrears.
Additional specialist services outside the scope of the retained service may be procured by the Contracting Authority using the agreed resource rates where required and subject to prior approval by the Contracting Authority.

Part 2 – Non-ICT Cyber Security Support Services

These services will be utilized on a drawdown basis in accordance with the requirements set out in this Specification.

This part will support non-ICT cyber security needs for business units for legislative obligations. This may include working with internal An Coimisiún teams that are tasked with implementing the Online Safety Framework (OSF), Digital Services Act (DSA) or any other relevant legislation.

The types of roles required under Part 2 are the same as Part 1, and are listed in Section 15.

5. Service Delivery Model

Proposed approach to Service Delivery and delivering a Partnership model
The role and requirements faced by Coimisiún na Meán are continuously evolving, and An Coimisiún is looking to deliver best-in-class solutions to support delivery of our mission. Coimisiún na Meán are looking for an experienced technical liaison and team to work in collaboration with existing third-party suppliers and the An Coimisiún's internal staff to support current implementations and to advise on Cyber Security matters as the An Coimisiún look to

deliver effective business solutions that continuously add value to the work of the An Coimisiún.

It is expected that the successful tenderer will have a close working relationship with An Coimisiún. With this type of partnership model of working in mind, An Coimisiún is interested in not only examples of where a tenderer has delivered these types of services (out lined in Part 1) successfully to other customers (covered by references) but how they went above and beyond obligations in meeting a high level of service delivery.
It is expected that in addition to an account manager role, the primary contract for An Coimisiún will be a technical liaison that can deal directly with requests from An Coimisiún or delegate them to the appropriate resources.

The tenderer teams will be working primarily with a small group within the ICT team. It is expected that most technical implementations will be undertaken by An Coimisiún's MSP however if the required expertise isn't in place then the tenderer will lead the implementation.

Coimisiún na Meán work in a hybrid manner, so this contract will include an element of in-person meetings (in addition to regular online meetings) at Coimisiún na Meán's main Offices in Ireland (Dublin 4) to include meetings for security recommendations, strategies, solution evaluations, audits, innovation and problem solving. That said, Coimisiún na Meán are supportive of near-shore delivery, provided that data protection rules are rigidly enforced while all data must reside within the EEA.

As outlined above, Coimisiún na Meán are seeking to engage with an organization that will operate a partnership model rather than in a traditional supplier/customer manner and we will look for the partner to be proactive and innovative in designing and delivering Cyber solutions that meet our ever growing and diverse business needs. Key requirements will include:

- A willingness to adapt to circumstances which may change frequently and/or at short notice
- A capability to ensure that Coimisiún na Meán delivers services in a secure, cyber resilient environment.
- An understanding of the ongoing mission of Coimisiún na Meán
- The ability to liaise closely with Third-Parties who are engaged to deliver Information Technology Solutions
- The ability to be proactive in helping Coimisiún na Meán be at the forefront of new technologies and/or delivery mechanisms.

6. Conflict of Interest

As Coimisiún na Meán is a regulator, it is essential that Tenderers demonstrate a clear, robust and transparent approach to the identification, disclosure, management and mitigation of actual, potential or perceived conflicts of interest. Tenderers must disclose any current, previous or proposed commercial, advisory, implementation or other relationships with organisations regulated by, supervised by, or otherwise engaged with Coimisiún na Meán that may give rise to an actual, potential or perceived conflict in the delivery of the Services. This includes relationships which may reasonably give rise to a perceived independence or

impartiality concerns, even where no formal conflict currently exists. Further information about these entities can be found on An Coimisiún's website.

Tenderers must clearly demonstrate the governance arrangements, organisational separation measures, reporting lines, confidentiality controls, ethical walls and escalation procedures that are in place to ensure the independent and impartial delivery of the Services. Particular attention should be given to the separation between security advisory/governance services and security implementation, managed service delivery, MDR/SOC services or other operational cyber security functions.

Tenderers should outline their formal conflict of interest policies and procedures, including how conflicts are identified, assessed, recorded, monitored, managed and escalated throughout the contract term. Tenderers should also confirm their commitment to ongoing disclosure obligations for any actual, potential or perceived conflicts arising during the duration of the Contract and confirm that Coimisiún na Meán will be notified immediately upon identification of any such conflict.

Tenderers should also provide details of how conflicts will be managed operationally on a day-to-day basis, including resource allocation controls, information segregation measures and governance oversight arrangements. Coimisiún na Meán reserves the right to assess the materiality of any disclosed conflict and, where necessary, require additional mitigation measures, resource separation arrangements or other appropriate controls.

All personnel assigned to the Contract shall be subject to appropriate confidentiality, ethics and conflict management obligations throughout the duration of the Contract. Failure to appropriately disclose or manage conflicts of interest may result in exclusion from the competition process, termination of the Contract or other proportionate contractual remedies.

7. Sustainability

Tenderers should provide clear and measurable information regarding the sustainability practices and initiatives that will directly support the delivery of the Services under this Contract. Responses should include details of how the Tenderer will minimise environmental impact through the proposed service delivery model, including the use of remote and hybrid delivery approaches, reduction of unnecessary travel, efficient use of technology infrastructure, and sustainable operational practices relevant to cyber security and ICT consultancy services. Tenderers should also outline any broader corporate sustainability initiatives, recognised environmental certifications or standards held, responsible supply chain practices, employee wellbeing and diversity initiatives, and governance measures that support sustainable and ethical service delivery.

8. Tendering Structure and Consortium Participation

Coimisiún na Meán are aware that not all requirements may be met by a single supplier and are therefore open to bids from consortia, including SMEs, who can demonstrate an innovative, proactive approach to delivering the service, provided only that Coimisiún na Meán

will deal with a single point of contact who will have the authority to address issues across the consortium.

SMEs are therefore encouraged to explore the possibilities of forming relationships with other SMEs or with larger enterprises to meet the financial, economic or technical capacity requirements of the competition, if required.
Tenderers may include individuals, partnerships, limited companies, groupings or any combination of the foregoing with or without legal personality. However, a grouping if successful will be required to establish legal personality to enter the framework agreement / contract.

Tenderers are reminded that they may rely on the resources of other entities to establish the requirements on condition that they can prove to the satisfaction of the Contracting Authority that they will have these resources at their disposal when necessary.

If the tender is from a consortium / joint venture, tenderers must ensure that all the relevant information is provided and where necessary, provide the information requested separately for each party. Relevant information relates to where a tenderer is relying on the resources to qualify (e.g. turnover, manpower, previous experience) and/or to deliver contracts. The consortium must appoint a single point of contact who will assume overall responsibility for delivery, and who is authorised to sign the framework agreement / contract on behalf of all consortia members. The Contracting Authority will not act as an arbitrator between members of consortia.

It is expected that each member of a consortium will have at a minimum, one of the qualifications listed above.

9. Support Hours

Regular Support will primarily be required from 08:00 – 18:00, Monday through Friday. In exceptional circumstances, including major incidents, outages or data breaches, support may be required outside these hours. Where additional specialist resources or sustained incident response support is required, this may be procured under the applicable day rates or specialist services pricing.

10. Governance & Reporting

Monthly and quarterly governance meetings should be scheduled to review performance, resource allocation, and overall contract management. Prospective partners should note the distinction between account management (strategic relationship and resource deployment) and contract management (administrative compliance and reporting), as the latter will be considered non-billable. The successful Tenderer may be required to agree reasonable service delivery performance measures, governance reporting requirements and escalation procedures with the Commission following Contract award.

The successful tenderer will report to the ICT Head of Security, or a nominated deputy and will work closely with the ICT team at Coimisiún na Meán.

The successful Tenderer shall provide reasonable transition assistance at Contract expiry or termination to support the orderly transfer of Services to the Commission or a replacement provider.

The successful Tenderer may also be required to support periodic audit, compliance or assurance reviews relating to the Services

11. Presentation Requirements

As part of the evaluation process, a presentation by the proposed technical liaison will be required. This will consist of a 20-minute presentation followed by a 10-minute question and answer session with the evaluation team and selected senior management representatives. The presentation will take place in person at Coimisiún na Meán's offices on Shelbourne Road, Dublin 4.

Only Tenderers who achieve the minimum qualifying threshold score in all applicable award criteria (excluding Cost and Sustainability) will progress to the Presentation stage of the evaluation process.

The Presentation will be evaluated solely under the published Presentation award criterion set out in Section 5.2. The Presentation will assess the Tenderer's proposed response to the scenario provided and will not be used to re-evaluate qualifications, certifications, experience or expertise already assessed under the written award criteria.

The Presentation topic will be issued by Coimisiún na Meán at least one week in advance of the scheduled Presentation date and will relate to a cyber security topic relevant to the Services being procured under this Contract. Tenderers should ensure that the proposed technical liaison and key personnel attending the Presentation are those proposed for delivery of the Services under the Contract

Tenderers should ensure that the Presentation supports and expands upon the submitted tender response and does not materially alter or contradict the submitted proposal, pricing structure or proposed resource model. Coimisiún na Meán reserves the right to seek clarification during the Presentation stage in relation to any aspect of the submitted tender response.

After the tender closing date, and once the written tender submissions have been evaluated, Tenderers progressing to Presentation stage will be provided with at least one week's notice of the proposed presentation schedule. The title, topic and format of the Presentation will be included with the presentation invitation.

12. Minimum Expected Deliverables and Outputs

The successful Tenderer will be expected to provide a combination of retained advisory services and optional specialist cyber security support services throughout the Contract term.

The following represents the minimum expected deliverables and outputs under the Contract. Tenderers may propose additional value-add services, governance measures or deliverables where considered beneficial.

Part 1 – CISO Advisory Service and ICT Cyber Security Services

- Review of current ISO 27001 aligned Policy and Standards identifying any gaps or potential improvement
- Develop a roadmap for assessment and remediation of An Coimisiún vs NIS2 with a view to being compliant.
- Quarterly review of our ICT risk register
- Weekly hybrid, and monthly in-person meetings with our cybersecurity team, to review ongoing progress, open actions/items, audit activities and any current/potential security issues
- Quarterly reporting and potential executive briefings on An Coimisiún's security posture

Part 2 – Non-ICT Cyber Security Support Services

- Generation of high-quality Statements of Work for any potential activities outlining the work to be done, expected deliverables, proposed team and timescale.
- Minimum of weekly meetings with internal teams to support any agreed activity
- Production of deliverables to support any agreed activity
- Final report documentation of any agreed activity

13. Service Delivery Principles

The successful Tenderer shall deliver the Services in accordance with the requirements set out within this Contract and Specification. The Services shall be delivered in a professional, proactive and collaborative manner, with a focus on supporting Coimisiún na Meán's operational, regulatory and cyber security requirements.

Tenderers should describe their proposed approach to service delivery, governance, stakeholder engagement, communication and continuous service improvement. Responses should focus on how the Services will be delivered and managed throughout the Contract term.

The Contracting Authority will evaluate Tenderers solely against the published award criteria and weightings. No additional marks shall be awarded for services, capabilities or offerings that are not expressly evaluated under the published award criteria

14. Service Scope and Resource Requirements

Tenderers shall provide the personnel, qualifications, experience and specialist expertise necessary to deliver the Services described within this Specification.

The proposed Technical Liaison / Lead CISO resource shall have a minimum of 10 years' relevant cyber security experience and shall hold at least one recognised professional certification such as CISM, CISSP or equivalent.

All specialist resources proposed under Part 2 of the Services shall possess qualifications, certifications and experience appropriate to the role being undertaken. Tenderers shall clearly identify the qualifications, certifications, experience and proposed responsibilities of each resource category.

15. Resource Categories

Tenderers shall provide pricing for the following resource categories:

- Lead CISO / Technical Liaison – Minimum 10 years' relevant experience and relevant CISM, CISSP or equivalent certification.
- Senior Cyber Security Consultant – Minimum 7 years' relevant experience.
- Security Auditor / Compliance Specialist – Minimum 5 years' relevant experience.
- Penetration Tester – Minimum 5 years' relevant experience and relevant CREST, CHECK or equivalent certification.
- Digital Forensics Specialist – Minimum 5 Years' relevant experience.
- Governance, Risk and Compliance Specialist – Minimum 5 Years' relevant experience.
- Data Protection Officer – Minimum 5 Years' relevant experience.
- Security Architect – Minimum 5 Years' relevant experience.

Tenderers shall provide curriculum vitae for all proposed key personnel and demonstrate how each individual satisfies the minimum requirements applicable to the proposed role.

Additional specialist services outside the scope of the retained service may be procured by the Contracting Authority using the agreed resource rates where required and subject to prior approval by the Contracting Authority.

APPENDIX 2 –TERMS AND CONDITIONS OF SUPPLY OF SERVICES

Attached Separately.

The Contract awarded following this competition shall be based on the applicable Office of Government Procurement Services Contract.

Tenderers should review the OGP contract documentation carefully and submit their Tender on that basis.