REQUEST FOR EXPRESSIONS OF INTEREST

Organisation of Eastern Caribbean States
Caribbean Digital Transformation Project (CARDTP)
Grant No.: IDA – D6520

Assignment Title: Consulting Services to Develop a Cybercrime Report, National Recommendations, and Cybersecurity Legislation for the Organisation of Eastern Caribbean States (OECS)

Reference No.: *LC-OECS COMMISSION-412915-CS-CQS*

The Organisation of Eastern Caribbean States (OECS) Commission has received funding from the World Bank toward the cost of the Caribbean Digital Transformation Project (CARDTP) and intends to apply part of the proceeds for Consulting Services to Develop a Cybercrime Report, National Recommendations, and Cybersecurity Legislation for the Organisation of Eastern Caribbean States (OECS).

The objective of the consulting services ("the Services") is to create a cybersecurity strategy for the region which will include offering national recommendations to the beneficiary countries, involving two key deliverables:

(i) Development of a comprehensive report on cybercrime for the Eastern Caribbean States
(ii) Based on the report on cybercrime, prepare draft cybercrime legislation in each beneficiary country.

The outputs must (i) reflect the common and respective needs, requirements, and objectives of Grenada, Dominica, Saint Lucia, and Saint Vincent and the Grenadines ("beneficiary countries") and (ii) promote regional harmonization and international good practices, including the Council of Europe's Convention of Cybercrime (the Budapest Convention) and be aligned with national and regional security strategies.

The assignment is expected to be undertaken over a period of one (1) year.

The OECS now invites eligible consulting firms ("Consultants") to indicate their interest in providing the Services. Interested Consultants should provide information demonstrating that they have the required qualifications and relevant

experience to perform the Services. The minimum required qualifications and experience are listed in section 4 of Terms of Reference (TOR). The details of the services required are available in the TOR which is available on the official website: www.oecs.int or can be obtained at the address given below.

The attention of interested Consultants is drawn to Section III, paragraphs, 3.14, 3.16, and 3.17 of the World Bank's Procurement Regulations for IPF Borrowers, Fifth Edition, September 2023 ('Procurement Regulations'), setting forth the World Bank's policy on conflict of interest.

To obtain the maximum degree of comparison among Expressions of Interest (EOIs) and facilitate the evaluation process, the EOI should be a maximum of 30 pages and include the following information included below:

- **Title page with name of firm submitting the EOI**: should contain name of firm (or joint venture and/or a sub-consultancy, if applicable), address, email, telephone, name of contact person and date of submission.
- **Expression of Interest**: including the firm's general and specific experience, similar assignments, curriculum vitae of the pool of experts, etc.

Consultants may associate with other firms to enhance their qualifications, but should indicate clearly whether the association is in the form of a joint venture and/or a sub-consultancy. In the case of a joint venture, all the partners in the joint venture shall be jointly and severally liable for the entire contract, if selected.

A Consultant will be selected in accordance with the Consultants' Qualification selection method set out in the Procurement Regulations.

Further information can be obtained at the address below during office hours 08:30 a.m. – 4:00 p.m. (0830 to 1600 hours).

Ms. Jenna Flavien
Procurement Officer
Caribbean Digital Transformation Project
OECS Commission
Morne Fortuné
P.O. Box 1383
Castries
Saint Lucia
Telephone: 758-455-6424/285-1980
Email: *procurementbids@oecs.int*

Copied to:
Mr. Imran Williams, *imran.williams@oecs.int*

An electronic copy of Expressions of Interest are to reach the OECS Commission by **May 27, 2024** addressed to:

Ms. Jenna Flavien, Procurement Officer
At the following email address:
procurementbids@oecs.int
copied to imran.williams@oecs.int

The email submissions should include the name and address of the Consultant and shall be clearly marked in the subject line as "**Expression of Interest – "Consulting Services to Develop a Cybercrime Report, National Recommendations, and Cybersecurity Legislation for the Organisation of Eastern Caribbean States (OECS)".**

Caribbean Digital Transformation Project
IDA – D6520

Scope of Services
Terms of Reference

Consulting Services to Develop a Cybercrime Report, National Recommendations, and Cybersecurity Legislation for the Organisation of Eastern Caribbean States (OECS)

May 2024

TABLE OF CONTENTS

1. PROJECT BACKGROUND

The the Organization of Eastern Caribbean States ("OECS") Commission and the Governments of Grenada, Dominica, Saint Lucia, and St. Vincent and the Grenadines are implementing the Caribbean Digital Transformation Project ("project") financed by the World Bank Group. This project, funded by the World Bank Group, is set to catalyse the development of the Eastern Caribbean's digital economy as a pivotal force for economic expansion, job creation, and enhanced public service delivery. With a comprehensive strategy comprising four main components, the project targets key barriers and opportunities for digital economy growth.

Furthermore, it is dedicated to ensuring that every person and business within the region can fully engage in an ever-evolving digital marketplace and society, equipped with necessary broadband access, digital financial services, and skills. By modernizing and digitizing the public sector, the project aims to upgrade service delivery and establish a robust digital culture throughout the Eastern Caribbean. It includes strengthening cybersecurity policies, capacity, and planning tools to better manage digital risks.

Additionally, the project will promote the adoption of technology to boost productivity in leading industries and stimulate the creation of digitally enabled jobs. It seeks to enhance regional integration and cooperation, harnessing economies of scale and scope to amplify the impact and cost-effectiveness of its actions. This will not only foster a competitive and integrated regional digital market to lure investments but also support the expansion of digital enterprises, offering them substantial growth opportunities.

Component 1.3 of the project, led by the Caribbean Community ("CARICOM") Implementing Agency for Crime and Security ("IMPACS,") focuses on cybersecurity and data protection (privacy) by improving the legal and regulatory framework, and strengthening institutional capacity. The aim is to establish an enabling environment that fosters trust in online transactions, enhance the security and resilience of digital infrastructure, promote cybersecurity awareness, and develop the capacity to protect against risks and vulnerabilities. The approach combines regional and national strategies to share knowledge, resources, and respond to challenges relevant to both local and regional contexts.

Significant technical assistance has been undertaken by IMPACS, with support from the European Development Fund, on cybercrime and cybersecurity legislation and policies. Key outputs include:

- Cybercrime Diagnostic Assessment Report for the CARIFORUM region;
- Cybercrime Legislation Budapest Comparative Analysis;
- Cybercrime Legislative and Policy Guidance Framework;
- CARICOM IMPACS Cybercrime Framework.

2. SCOPE OF SERVICES

Within the scope of Component 1.3 of the project, the OECS Commission plans to contract a firm tasked with creating a cybersecurity strategy for the region ("Consultant.") This strategy will include offering national recommendations to the beneficiary countries, involving two key deliverables:

(iii) Development of a comprehensive report on cybercrime for the Eastern Caribbean States

(iv) Based on the report on cybercrime, prepare draft cybercrime legislation in each beneficiary country.

The outputs must (i) reflect the common and respective needs, requirements, and objectives of Grenada, Dominica, Saint Lucia, and Saint Vincent and the Grenadines ("beneficiary countries") and (ii) promote regional harmonization and international good practices, including the Council of Europe's Convention of Cybercrime (the Budapest Convention) and be aligned with national and regional security strategies. The Consultant must also consult with various national and regional stakeholders.

Overall, the delivery will provide actionable instructions for developing a national cybercrime framework. The OECS Commission seeks a firm with a strong track record of the activities herein.

The scope of services of the Consultant is as follows:

Output #1: Development of a report on the state of cybercrime and existing legislative framework for the Eastern Caribbean States

<u>Cybercrime Report for the Eastern Caribbean States</u>

Research and Data Collection:

- Conduct comprehensive research on cybercrime trends, threats, and challenges specific to the Eastern Caribbean States.
- Collect data from government agencies, law enforcement agencies, cybersecurity organizations, relevant government agencies (e.g., sectoral regulators) academic institutions, civil society, private sector, and international partners.

Stakeholder Engagement:

- Engage relevant stakeholders and government agencies, including Chief Parliamentary office, Office of the Attorney general, law enforcement agencies, judiciary, prosecutors, regulatory bodies, private sector organizations, civil society, academia, and international partners, etc.
- Organize consultations, workshops, and interviews to gather insights, perspectives, and recommendations.

Analysis and Review:

- Analyze the data to evaluate the state of cybercrime in the Eastern Caribbean States.
- Review existing laws, regulations, and policies on cybercrime prevention, investigation, prosecution, international cooperation, and support for victims.
- Assess the effectiveness of existing legal frameworks and cybersecurity measures.
- Identify areas needing legislative reform to strengthen legal frameworks against cybercrime.

Recommendations:

- Develop recommendations for a draft Cybercrime legislation for adoption by beneficiary countries.

Report Compilation:

- Compile findings, analyses, and recommendations into a comprehensive report with draft text for a Cybercrime legislation annexed.
- Present the report and draft text for beneficiary countries to the OECS Commission.

Output #2: Based on the report on cybercrime and the draft text, propose cybercrime legislation in each beneficiary country.

Legal Framework Analysis:

- Identifying specific legislative areas that require development, amendment, harmonization, and standardization across each beneficiary country. This effort must advance key project activities, including alignment with the CARICOM Cyber Security

and Cybercrime Action Plan, the Harmonized Framework Document, and adherence to international best practices, such as those outlined in the Budapest Convention.

Stakeholder Consultation Preparation:

- Organize and conduct consultations (in-person whenever possible) with national and regional stakeholders to develop, present, and review the draft legislation in each beneficiary country. These sessions should include cybersecurity and cybercrime investigation professionals, legal drafters, and practitioners, as well as representatives from the private sector and civil society.
- Establish a comprehensive list of participants for national consultations, engaging with stakeholders such as cybersecurity experts, cybercrime investigators, prosecutors, judiciary members, legal professionals, private sector representatives, and civil society groups, underlining the importance of including a wide array of viewpoints for a comprehensive and inclusive legislative drafting process.

Draft Legislation:

- Develop draft legislation, amendments to current laws, or both as necessary, in the beneficiary states, guided by the findings from consultations and the dual criminality standards for international cooperation. The proposed legal changes should comprehensively address:
  - Substantive law, focusing on criminal offenses.
  - Procedural law, including aspects such as the admissibility of electronic evidence, procedural powers and measures, attribution, jurisdiction, international cooperation, and legal safeguards.
  - The institutional framework required to support and enforce these laws.

Adoption and Implementation Report:

- Submit a comprehensive report with recommendations for the legislation's adoption and implementation, including potential risks and mitigation strategies.

National Champions Identification:

- Identify key national figures to champion the draft legislation towards enactment.

Standard Operating Procedures (SOPs) for Database Access:

- Develop Standard Operating Procedures for data entry and to guide access to a relational Cybercrime Legislation and Cybersecurity Policy Database located at CARICOM IMPACS (RIFC) Regional Intelligence Fusion Centre. Access to this regional database at CARICOM IMPACS will provide beneficiary Member States the ability to track changes to Regional and International Cybercrime Legislation and Cybersecurity Policies.

3. ASSUMPTIONS UNDERLYING THE PROJECT

The following assumptions are made for the success of the project:

- Member States will cooperate and participate in project activities and provide information and feedback in a timely manner.
- Whenever possible, consultations shall be conducted in person to facilitate direct engagement. When physical travel is not feasible, virtual consultations will be organized as a secondary option to ensure the continuity of project activities. The Consultant is responsible for adapting to potential constraints, such as travel restrictions, by making alternative arrangements to maintain the project's momentum and robust stakeholder engagement under all circumstances.
- Adequate in-country consultations will be undertaken by the Consultant with all national entities. This will be a whole-of-society and whole-of-government approach,

engaging a wide range of stakeholders from various sectors to gather diverse insights and ensure the recommendations are practical and widely supported.

- Each submission must be acceptable to CARICOM IMPACS, relevant beneficiary countries, the CARICOM Secretariat, and the OECS Secretariat. This implies that the project outcomes must align with international standards and regional priorities, enhancing cooperation and implementation feasibility.
- Wherever possible, project deliverables will be informed by, and incorporate, feedback from consultations, ensuring that the draft legislation, action plans, and reports reflect the inputs from all engaged stakeholders.
- Quality control measures, such as peer reviews and stakeholder validation of findings, will be employed at each stage to maintain high standards of work.
- The project is premised on the assumption that its outcomes will adhere to international best practices, such as those outlined in the Budapest Convention, ensuring relevance and facilitating international cooperation.
- The project assumes an emphasis on building local capacity and ensuring the sustainability of its outcomes through training sessions, workshops, and the development of SOPs for ongoing activities.

4. CONSULTANT REQUIREMENTS AND QUALIFICATIONS

The Consulting Firm must be able to perform all tasks specified in the TOR and have the relevant experience outlined below:

- The selected Consulting Firm should have international repute and a strong and demonstrated track record in cybersecurity and cybercrime frameworks.

- At least one successfully completed similar assignment during the past five (5) years, including drafting cybercrime legislation.

- At least five (5) years' experience supporting the implementation and enforcement of a cybersecurity framework.

Qualifications of the Consultant's Team

The Consultant's team should be composed of at least the following members:

Team Leader

- A lawyer with admission to practice, with at least eight (8) years of proven experience in drafting, reviewing, and advising on legislation, specifically in the areas of cybersecurity and cybercrime.
- Proven experience in offering legal implementation support within the public sector, with a focus on cybercrime and cybersecurity policies, would be highly beneficial.
- Experience with the regulatory aspects of cybersecurity and cybercrime, along with familiarity with international best practices in the field, including adherence to frameworks like the Budapest Convention, would be a significant advantage.
- Knowledge of the CARICOM Cyber Security and Cybercrime Action Plan, the Harmonized Framework Document, and familiarity with the legal and regulatory environments of Eastern Caribbean States regarding cybersecurity and cybercrime.

Project Team Members

Team member(s) with multidisciplinary training related to the tasks, including at least:

- A lawyer with admission to practice, with at least five (5) years of experience in cybersecurity and cybercrime.
- A policy specialist with at least five (5) years of experience in cybersecurity strategy and policy development and implementation.
- Training in the field of security and/or regional expertise on cybercrime/cybersecurity operations including the evolving policy and regulatory framework; additional training in areas such as cybercrime investigations, cybersecurity, data protection/privacy, security technology, and intellectual property is beneficial.
- Advanced technical qualifications and certifications are highly valued, but not preferred, including: Certified Ethical Hacker, Certified Information Security Manager, and Certified Information Systems Security Professional.
- Skills in cybersecurity risk management, national security matters, investigations, and intelligence and international relations.

5. ASSIGNMENT DURATION, DELIVERABLES AND PAYMENT SCHEDULE

The estimated duration of the assignment is one (1) year. The expected deliverables, and indicative timeline and payment schedule are set out below:

Timing	**Outputs relating to the Scope of Services**	**Deliverable**	**Contract Amount (%)**
Month 1	Output 1	Inception Report, at minimum (a) analyzing existing legal frameworks in beneficiary countries and identifying specific areas which should be developed, amended, harmonised and standardised for each beneficiary State; (b) providing an overview of the methodology and approach, any potential challenges and strategies to mitigate those risks; (c) identifying key stakeholders and partners who will be involved in the project, and outline a plan for engaging with them throughout the process, and (d) providing a timeline for the project, including key milestones and deliverables, and outline the resources required to successfully complete the project.	15%
Month 4	**Output 2**:	Report on cybercrime for the Eastern Caribbean States and regional action plan	35%
Month 11	**Outputs 3**	Final drafts legislation indicating and/or amendments/enhancements	50%

		to existing cybercrime laws of beneficiary states.	

For each deliverable, the Consultant must (i) conduct stakeholder consultation(s) and identify key stakeholders for participation, (ii) provide a report on the consultation and make necessary revisions, and (iii) submit for approval by IMPACS, relevant beneficiary country, or both.
The Consultant must consult with a number of national and regional stakeholders including, but not limited to:

- Attorneys General Chambers
- Ministries of Legal Affairs
- Ministries with responsibility for ICT
- Parliamentary Counsels and parliamentarians
- Law Commissions, Legislative Drafting Departments and members of the legal fraternity
- National Telecommunications Regulatory Commission
- CARICOM IMPACS
- OECS Commission
- CARICOM Secretariat
- Organisation of American States
- Caribbean Telecommunications Union
- Eastern Caribbean Telecommunications Authority (ECTEL)

6. REPORTING

The Consultant will report to IMPACS and OECS. The Consultant must prepare succinct and relevant documentation and submit monthly and quarterly reports on project status. The Consultant must keep records and a database of all collected legal and policy sources related to the analysis and make them available per request of OECS. The quarterly reports must provide details on the status of achievements, challenges, risks, and recommendations for project implementation. They will be used for mid-course corrections based on the nature and scope of the project. These will convey results, alternative solutions, and major decisions that need to be made.