CARIBBEAN DIGITAL TRANSFORMATION PROJECT
IDA Credit P171528

REQUEST FOR STATEMENT OF CAPABILITY
Support for Design and Development of the Cyber Security Agency
Ref. No.: GD-PCU - GRENADA-257128-CS-INDV

The Government of Grenada, Ministry of Finance, Economic Development, Physical Development, and Energy invites suitably qualified individuals to apply for the position of **Support for Design and Development of the Cyber Security Agency under** the Caribbean Digital Transformation Project, funded by the World Bank.

Project Summary
The Government of Grenada is preparing to implement a digital transformation project, financed by the World Bank Group. The Caribbean Digital Transformation Project (called "the project" going forth) comprises four components that address key bottlenecks and harnesses opportunities to develop the Eastern Caribbean Digital Economy as a driver of economic growth, job creation and improved service delivery.

The project aims to ensure that each individual and business within the region is empowered with the access to broadband, digital financial services, and skills needed to actively participate in an increasingly digital marketplace and society. It leverages public sector modernization and digitization to improve service delivery and to drive creation of a digital culture across the region. To support the improved management of digital risks, the project will bolster cybersecurity policy, capacity, and planning tools in the region.

The project will facilitate technology adoption to improve productivity of flagship industries and create demand for digitally enabled jobs. It aims to foster regional integration and cooperation to capture the economies of scale and scope required to increase impact and value for money of the project interventions and to create a more competitive, seamless regional digital market to attract investment and provide room for growth of digital firms.

Brief Overview of Scope of works:

The consultant will provide strategic direction to the Government of Grenada, through the Ministry of ICT, towards the establishment of a National Cyber Security Agency and institutionalization of the National Cyber Emergency Response Team (nCSIRT) which has the authority to provide the necessary cyber security services to the nation.

National Cyber Security Agency
A. Assessment
I. Review the current Cyber Environment in Grenada, specifically based on the latest assessment report provided by the Organization of the American States.

II. Review/assess the current operational capabilities of internal staff of the Government of Grenada (in the context of institutionalizing a CSA)
III. Consult with relevant stakeholders to ensure the formulation of the CSA adopts participatory development process.
IV. Provide recommendations that are suitable for the development of the agency, specifically noting the concerns of the Ministry of National Security, regarding Cyber Security.

B. Cybersecurity Agency Organizational and Operational Framework
I. Develop a National Cybersecurity Strategy and Cyber Risk Management Program for the next 5 years that should be implemented by the CSA.
II. Develop an operational CSA/CERT framework that includes Conceptual, organizational model, operational model, legal/regulatory framework, risk management guidelines and whistleblower guidelines. The models must be demonstrated to ensure their practicality and applicability to national context and include clear guidance on incident handling, communications, disaster recovery plan.
III. Establish the Operational Standards and Procedures Manual for the national CERT/CSA which must include midterm work plan, roles and responsibilities matrix and terms of reference of core staff, financial sustainability plan (CapEx and OpEx), and localization of regionally developed trust and transparency frameworks. The manual must include, as an include section or separate documents cyber normative which covers procedures on community engagement management, confidentiality agreement, membership agreement, information classification normative, security normative, acceptable use of the information systems and use of cryptographic controls

C. Procurement and Physical Conditioning of the CSA
I. Design a procurement plan in consultation with the designated project oversight officer for the purchase and implementation of technologies and services for the CSA, including hardware, licenses, and possible consultancy.
II. Develop terms of references for contracting a provider to adequately outfit the physical facilities and implement necessary hardware and software to support the services for the operations of the CSA.
III. Identification and evaluation of potential providers involved in the technical deployment of necessary services required by the CSA/CSIRT (private companies, consultants, or other)
IV. Support and provide guidelines in the acquisition process of CSA's equipment, including servers, office equipment, network devices, licenses, etc.
V. Support activities for the physical conditioning of the Data Center and offices space of the CSA staff.
VI. Support activities for the deployment of technological infrastructures of the CSA including servers, networks and backups.

D. Capacity Building and Knowledge Transfer

I. Develop the organization's (CSA) functional statement, vision and mission. Its human resource needs along with the job functions for each of the proposed roles in consultation with the Department of Public Administration and the Ministry of ICT as key stakeholders.
II. Provide training and knowledge sharing to identified staff and security resources and or provide a list of recommendations of courses or certifications standards that staff at the agency, this aims to ensure optimal operational capacity is viable for the CSA and CIRST staff in Grenada.
III. Developed Terms of Reference (TORs) document to assist with the hiring of core staff members.
IV. Provide training to selected staff on ALL frameworks, models and manuals developed under this consultancy.
V. Provide support for the monitoring and supporting activities for the deployment of various systems such as the website, incident management systems, notification systems and configuration of cyber-threat intelligence feeds subscriptions.
VI. Supervise and provide handholding support to management of the CERT/CSA for its initial two months of operations to ensure institutionalization of operational procedures and manuals are implemented as envisioned.

V. Required Experience and Qualifications

Evaluation will be done based on the following criteria for all consultant:

1. The consultant must also present proven experience with past work, specifically in the last five (5) years related to the matter of establishment of Cyber security team – CIRST/CERT/CSA
2. At least a BSC in the field of ICT or IT/IS security.
3. Have documentary evidence or experience in the design and development of CERT/CIRST/CSA or similar organizational and operational structure.
4. Evidence where consultant has provided guidance toward the implementation of a CERT/CIRST/CSA plans within a private or public sector agency.
5. Have documentary evidence and knowledge of NIST develops cybersecurity standards, guidelines, best practices and other related framework such as:
    - ISO/IEC 27005 Information Security Risk Management.
    - Certified in Risk and Information Systems Control (CRISC)
    - Certified Information Security Manager (CISM).
    - Certified Information Systems Auditor (CISA).
6. Have directed training or provided training on policy level cyber security and information protection.
7. Have provided or directed training for entry level training in cyber security that leads to industry level certification.
8. Has documentary evidence or reference of work, in the area of advisory services of similar nature.

VI. Reporting

The consultant shall report to the Project Manager within the Digital Transformation Office and adhere to all other reporting requirements as outlined in section 4 (Deliverables)

VII. Contract Duration

The contract is expected to be executed over 1 calendar year.

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" July 2016 revised November 2017, July 2018, and November 2020 ("Procurement Regulations"), setting forth the World Bank's policy on conflict of interest.

A Consultant will be selected in accordance with the Individual Consultant Selection (ICS) method set out in the Procurement Regulations.

Further information and Terms of Reference can be obtained at the address below during office hours of 8:00 a.m. and 4:00 p.m. Monday to Friday or via e-mail to imi@gov.gd.

Project Manager
Caribbean Digital Transformation Project
Ministry of Finance, Economic development, physical development, public utilities, and Energy
Botanical Gardens, Tanteen, St. George
Tel: 1-473-423-1109

Qualified and interested persons should submit an application in via e-mail along with a resume and cover letter, on or before September 16, 2022 to:

Re: Support for Design and Development of the Cyber Security Agency
E-mail: imi@gov.gd , procurementofficer@procurement.gov.gd,