Annex 1

Caribbean Digital Transformation Project

IDA – 6685DM

Terms of Reference

Support for Development of National Cybersecurity Capability

DM-MPWDE-301830-CS-INDV

August 2022

TERMS OF REFERENCE FOR SUPPORT FOR DEVELOPMENT OF NATIONAL CYBERSECURITY CAPABILITY

A. INTRODUCTION

1.**Project number**: P171528	2. **Organization name**: Ministry of Public Works and the Digital Economy (MPWDE)
3**. Project name**: Caribbean Digital Transformation Project (CARDTP)	3.1. **Position**: Support for Development of National Cybersecurity Capability
4. **Contract duration**: 12 months Beginning: September 30, 2022 (Indicative) End: September 29, 2022	4.1 **This position reports to**: Project Manager

5**. Project Background**:

The COVID-19 pandemic, and the restriction to face-to-face interactions it entailed, marked a historic milestone in the transition of daily life to digital environments. In Latin America and the Caribbean (LAC) alone, it drove the expansion of digital commerce at an annual growth rate of 31% per year until 2025, and the adoption of technologies such as the 5G network, with an estimated penetration of approximately 86 million users in the region by the same date. As our daily life activities increase in digital ecosystems, cyber threats do. The tech company Microsoft revealed that in 2021 cyberattacks in the region increased by 24% year-on-year, presenting 35,700 phishing attempts through emails. Exploiting vulnerabilities, both people and their devices are one of the main opportunities for cybercriminals to carry out attacks.

Due to the increase in these cyber-attacks, and the growing risks in cyberspace, establishing a Computer Emergency Response Team (CERT) that can manage coordinated responses, and have a national monitoring role of the state of threats, is necessary. Its establishment will enable cybersecurity to be addressed and cyber resilience to be developed as a priority practice in all social and economic spheres.

Sitting halfway along the Eastern Caribbean archipelago, Dominica is located just a few miles from Martinique to the south and Guadeloupe to the north. Stretching 751 km^2 (290 square miles), Dominica boasts 148 km (91 miles) of coastal line. Dominica's official name is the 'Commonwealth of Dominica,' which is mostly referenced in official communications and to further distinguish the island from the Dominican Republic, its northerly Caribbean sister. Dominica is the most northernly of the Windward Islands grouping.

The Caribbean Digital Transformation Project (CARDTP) is funded by the World Bank and aims to enhance the use of technology in the public sector as well as the private sector to conduct business transactions, build a robust and resilient IT infrastructure and to develop modern platforms to facilitate and enhance these business transactions. The development objectives are to contribute to increased access to digital connectivity, digital public services and the creation of technology enabled businesses and jobs in Dominica.

National-level activities are financed from an IDA credit to Dominica in the amount of SDR20,500,000 (equivalent to US$28.0 million). The Caribbean Digital Transformation Project (called "project" going forth) comprises four components that address key bottlenecks and harness opportunities to develop the Eastern Caribbean Digital Economy as a driver of growth, job creation and improved service delivery.

The Program is also financed through a regional IDA grant and implemented by a regional Project Implementation Unit (RPIU) housed at the Organisation of Eastern Caribbean States (OECS). RPIU will work with other regional institution stakeholders as relevant depending on the technical area being supported. Regionally implemented activities will focus on strengthening the enabling environment to promote investment, competition, and innovation in telecoms and digital financial services, regional cybersecurity collaboration, and a modernized and harmonized data protection and privacy regime across the region.

It aims to ensure that every individual and business in Dominica 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 drive the creation of a digital culture across Dominica.

To support the improved management of digital risks, the project will bolster cybersecurity policy, capacity, and planning tools in the region. It will facilitate technology adoption to improve the 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 the 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.

A brief description of the project components is as follows:

Component 1: Digital Enabling Environment

This component will support the development of a positive enabling environment for Dominica's digital economy that drives competition, investment and innovation while promoting trust and security of online transactions. It will focus on legal, regulatory and institutional reforms to support the modernization of the telecommunications and digital financial services sectors while mitigating growing risks of a digital economy, including cybersecurity and data protection and privacy.

1.1 - Telecommunications: Legal and Regulatory Environment, Institutions and Capacity Support

1.2 - Digital Financial Services: Legal and Regulatory Environment, Institutions, and Capacity

1.3 - Cybersecurity, Data Protection and Privacy: Legal and Regulatory Environment, Institutions and Capacity Support

Component 2: Digital Government Infrastructure, Platforms and Services

This component will support public sector modernization, resilience and delivery of digital public services to individuals and businesses. It will aim to ensure that Dominica has put in place the core infrastructure, platforms, institutions and human capacity needed to efficiently and effectively manage internal government operations, and to build on these core enablers to make public services widely accessible online from anywhere within the country, region or across the globe. It will also prepare Dominica's government for deeper interconnectivity and interoperability of data and information systems across borders to smooth administration of regional trade, immigration and other services. Finally, it will aim to ensure continuity of government operations and services, enable real-time data driven decision making and ability to rapidly target and deliver payments and social services to citizens and businesses in the event of natural disasters.

2.1 – Development of Cross-Cutting Enablers of Digital Government Operations and Services
2.2 - Government Productivity Platforms and Citizen-Centric Digital Services

Component 3: Digital Skills and Technology Adoption

This component aims to better equip individuals and businesses in Dominica for the jobs and economy of the future and to spur innovation and productivity growth. It aims to create a pool of advanced digital talent to better position Dominica to attract investment by digital firms. It takes a comprehensive supply and demand side approach, supporting greater technology adoption and utilization of digitally enabled business models to drive demand for newly skilled employees and well as making connections with global employment opportunities through online working platforms.

3.1 - Workforce-Ready Digital Skills
3.2 - Technology Adoption

Component 4: Project Implementation Support

This component includes support to the Project Implementation Unit (PIU) for the implementation and management of national level project activities, including for staffing of the PIU, capacity building and training initiatives as well as recruitment of a technical advisory and implementation support firm. Key technical functions to be supported can include but will not be limited to project manager, technical specialists, procurement specialists, financial management specialist, environmental and social specialists, monitoring and evaluation and communications.

B. INSTITUTIONAL ARRANGEMENTS

The Project will be implemented by the Project Implementation Unit (PIU) of the Ministry of Public Works and the Digital Economy (MPWDE). The PIU will be responsible for the overall implementation of the Project with emphasis on reporting and monitoring and evaluation, financial management, contracts management, safeguards oversight, and procurement.

The PIU will report directly to the Project Steering Committee for the lifetime of the project. It will be responsible for coordinating and managing all the technical aspects of the project, facilitating inter-ministerial coordination, and implementing digital initiatives across the various

Ministries, Departments and Agencies (MDAs) of the GoCD. The PIU will support the development of key policies and regulations and inter-agency coordination to enable consensus building together with other key agencies like the ICT Unit and the Digital Transformation Unit of the GoCD. Core technical responsibilities include the adoption of digital technologies, effective coordination of departmental information system development and implementation. The Project Steering Committee will determine if technical committees are required for policy formulation and convene such committees as necessary (i.e.; for Cybersecurity, Data Protection and Privacy, Service Delivery, ePayments, Digital Identity, Interoperability, etc.). The PIU, with guidance and support from the management firm, will also be responsible for promoting change management practices and stakeholder engagement, developing effective programs for digital Government skills development, knowledge exchange and awareness-raising.

The consultant is expected to work with the PIU to ensure that Component 1 is executed in order to build capacity for the sustenance the digital transformation agenda beyond the life of the Project.

C. FUNCTIONS

Key duties of this position:	The Cyber Security Consultant will assist with planning, designing, and implementing the Computer Emergency Response Team (CERT). Consultant shall be overseeing the rollout of National Cyber Security Operation Center (CSOC) in Dominica for CERT to operate and function. This shall entail working on threat intelligence, evaluating the risks and issuing advisories to affected organizations, sectors, government agencies and public in general.

Responsibilities

Support for development of national cybersecurity capability

The consultant will support the delivery of activities primarily under Component-1 and be responsible for the management and oversight of the security aspects under the Caribbean Digital Transformation Project, including drafting business case, Request for Proposal (RFP), Terms of Reference (TOR), and monitoring the onboarded vendor implementing CSOC.

The activity of the consultant is organized in the following tracks:

Track 1

- Undertake the necessary national consultations with relevant stakeholders to conduct a national incident response needs assessment. This will include but not be limited to,
  - Methodology for the consultations
  - Development of relevant questions
  - Coordination of national point of contact with government

    - Facilitate stakeholder discussions (virtual or in-site in coordination with the Government)
- Prepare assessment report that address the existing situation to determine reasons, needs and conditions for the creation and establishment of a CERT.

Track 2

- Design a work plan, including timelines and milestones, for the establishment and implementation of a National CERT based on the "Assessment for Readiness report" elaborated by the OAS-CICTE Cybersecurity Program [1].

- Establish and coordinate a working group with the Project Manager-PIU for the implementation of a National CERT in Dominica.

- Develop a high-level budget that takes into account the implementation and sustainable operations of the CERT for 24 months that takes into account CERT operational procedures, work plan, roles and responsibilities matrix, financial sustainability plan (CapEx and OpEx), and localization of regionally developed trust and transparency frameworks.

- Support the development of a preliminary mandate for a National CERT in Dominica.

Track 3

- Develop documentation necessary for the operation of the National CERT, including but not limited to strategy, conceptual, membership, community engagement, organizational, operational frameworks, services, and applicable legal framework.

- Design a procurement plan in consultation with the Project Manager-PIU for the purchase and implementation of technologies and services for the CSIRT, including hardware, licenses, and possible consultancy.

- 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 CERT.

[1] OAS-CICTE Cybersecurity Program to provide Consultant with links to some of the resource material to be consulted during the consultancy

- Identification and evaluation of potential providers involved in the technical deployment of the CERT (private companies, consultants, or other).

- Provide weekly updates to the Project Manager-PIU and incorporate feedback to the plan (by email or virtual meetings, as determined between the Consultant and Project Manager-PIU).

Track 4

- Develop terms of references for staff resources for the CERT (full-time human resources as agreed based on the plan described above).

- Support and provide guidelines in the acquisition process of CERT's equipment, including servers, office equipment, network devices, licenses, etc.

- Support and conduct interviews of candidates for staff positions in the CERT.

- Organize technical meetings and provide technical requirements to the company or consultants involved in the technical deployment of the CERT.

- Provide weekly updates to the CICTE Cybersecurity Program designated officer and the government designated Project Manager-PIU and incorporate feedback to the plan (by email or virtual meetings, as determined between the designated project oversight officer and the Cybersecurity Program)

Track 5

- Conduct monitoring activities and provide technical guidance for the physical conditioning of the Data Center and offices spaces of the CERT.

- Conduct monitoring activities and provide technical guidance for the deployment of technological infrastructures of the CERT, including servers, networks and backups.

- Support and develop procedure manuals on the services and processes of the National CERT, including community management, confidentiality agreements, incident handling, communications, disaster recovery plan, financial plan, etc.

- Provide weekly updates to the designated project oversight officer and the CICTE Cybersecurity Program designated officer and incorporate feedback to the plan (by email or virtual meetings, as determined between the Consultant and the Project Manager-PIU).

Track 6

- Conduct monitoring activities for the physical conditioning of the Data Center and offices spaces of the CERT.

- Conduct monitoring activities for the deployment of technological infrastructures of the CERT, including servers, networks and backups.

- Support and develop procedure manuals on the services and processes of the National CERT, including community management, confidentiality agreements, incident handling, communications, disaster recovery plan, financial plan, etc.

- Provide weekly updates to the designated project oversight officer and CICTE Cybersecurity Program designated officer and incorporate feedback to the plan (by email or virtual meetings, as determined between the Consultant and designated Project Manager-PIU)

Track 7

- Conduct monitoring and supporting activities for the correct deployment of common services for essential operations of the CERT.

- Conduct monitoring and supporting activities for the correct deployment of incident management systems of the CERT.

- Conduct monitoring and supporting activities for the correct deployment of email services and an official website of the CERT.

- Conduct monitoring and supporting activities for the correct deployment of notification systems and monitoring services of the CERT.

- Conduct monitoring and supporting activities for the initial configuration of cyber-threat intelligence feeds subscriptions.

- Provide weekly updates to the designated project oversight officer and CICTE Cybersecurity Program designated officer and incorporate feedback to the plan (by email or virtual meetings, as determined between the Consultant and Project Manager-PIU)

Track 8

- Conduct monitoring activities for the integration of the CSIRT with OAS CSIRT Americas Network services.
- Conduct testing and troubleshooting activities in services deployed in the CSIRT.
- Prepare and provide training for the staff of the CSIRT on the use of the services deployed.
- Provide weekly updates to the designated project oversight officer and CICTE Cybersecurity Program designated officer and incorporate feedback to the plan (by email or virtual meetings, as determined between the Consultant and Project Manager-PIU).

Track 9

- Prepare and provide training for the staff of the CERT on the use of the services deployed.
- Develop an executive presentation with key highlights of the CERT establishment and implementation.
- Participate in promotion activities (TBD) to launch the National CSIRT of Dominica in consultation and agreement with the designated project oversight officer.
- Provide weekly updates to the Project Manager-PIU and CICTE Cybersecurity Program designated officer and incorporate feedback to the plan (by email or virtual meetings, as determined between the Consultant and Project Manager-PIU).

C. REQUIREMENTS

Education	• Bachelor’s degree in business management or a related field is required, an MBA will be an asset.
Work experience & skills	- Bachelor’s degree in Computer Science, Electronics or in a related field, an MBA, will be an asset - Experience with national cyber security and resilience strategy - Experience in implementing Cyber Security Operation Center, including vulnerability management programs, incident response and recovery

	- Proficiency in Mitre’ Cyber ATT&CK framework, NIST (National Institute of Standards & Technology) Cyber Security Framework, Centre for Internet Security (CIS) Top 20 controls, CoBIT framework - Experience in managing protection plans for Critical Information Infrastructure at the sector or national level - A minimum of fifteen (15) years of experience in the cyber security solution architecture and engineering - Should possess CISSP (Certified Information Systems Security Professional) or Certified Information Systems Manager (CISM) credentials. PMP (Project Management Professional) and TOGAF (The Open Group Architecture Forum) certification shall be highly preferable. - Work collaboratively with CERT organizations in the region and globally to thwart cyber threats - Good interpersonal skills and ability to establish and maintain effective partnerships and working relations with various industry bodies and government agencies - Excellent negotiation skills
Language skills	High proficiency in spoken and written English
	High proficiency in MS Office (Word, Excel, PowerPoint, MS Project etc.) and excellent web navigation skills
Other skills	- High professional and personal integrity - Effective communication skills - Ability to submit information in a clear, concise manner and formats suitable for non-specialists - Strong analytical and problem-solving skills and proven ability to apply these in carrying out operational tasks identifying issues, presenting findings/ recommendations and contributing to the resolution of sector and country issues - Capacity to work simultaneously on a variety of issues and tasks, independently adjusting to priorities and achieving results with agreed objectives and deadlines - Ability to use one’s initiative and be proactive - Ability to be flexible with work assignments - Ability to stimulate and manage change and develop strong teams - Ability to uphold ethical standards - Familiarity with the World Bank environmental and social safeguards - Strong interpersonal skills and ability to work effectively with internal/external partners - Excellent communication and interpersonal skills - Ability to work both independently and collaboratively in a team

D. EVALUATION CRITERIA

- Bachelor's degree in Computer Science, Electronics or in a related field, an MBA will be an asset
- A minimum of fifteen (15) years of experience in the cyber security solution architecture and engineering
- Should possess CISSP (Certified Information Systems Security Professional) or Certified Information Systems Manager (CISM) credentials
- The Consultant should submit his/her detailed CV in World Bank format with a detailed description of his/her experience, projects/work undertaken, etc. The world bank format is placed at Annexure-A

E. CONTRACT DURATION AND ESTIMATED TIME INPUT

The assignment will be on a contractual basis for one (1) year in the first instance and can be renewed at the sole discretion of the Project Manager for another six months.

Annexure-A

World Bank CV Template

1. **Surname:**
2. **First Name:**
3. **Date of Birth**:
4. **Profession:** **Nationality**:
5. **Education**:
   -
6. **Membership of Professional Associations**:
   -
7. **Other Training**:
   -
8. **Countries of Work Experience:**
   -
9. **Languages:**
10. **Employment Record (Add rows as required)**:

From:
Employer:
Position Held:
Summary:

From:
Employer:
Position Held:
Summary:

From:
Employer:
Position Held:
Summary:

From:
Employer:
Position Held:
Summary:

From:
Employer:
Position Held:
Summary:

11. Work undertaken that best illustrates EIA related work (clearly showing role played, duration of input, complexity of work undertaken, and core competencies) **(Add rows as required)**	
Name of assignment or project: Year: Location: Client: Main Project Features: Positions held: Activities performed:	
Name of assignment or project: Year: Location: Client: Main Project Features: Positions held: Activities performed:	
Name of assignment or project: Year: Location: Client: Main Project Features: Positions held: Activities performed:	