TC Document

I. Basic Information for TC

▪ Country/Region:	REGIONAL
▪ TC Name:	Strengthening Cybersecurity Policy and Incident Response in the Caribbean
▪ TC Number:	RG-T4452
▪ Team Leader/Members:	Nowersztern, Ariel (IFD/ICS) Team Leader; Paz Gonzalez, Santiago (IFD/ICS) Alternate Team Leader; Reyes, Javier Ramiro (IFD/ICS); Ruddock, Sheries Alethea (CCB/CCB); Wilks, Jason Malcolm (IFD/ICS); Muente Kunigami, Arturo (IFD/ICS); Bonilla Merino Arturo Francisco (LEG/SGO); Martinez, Ynty Koyllor (IFD/ICS); Jordan, N. Maria (CCB/CCB); Bordese Maria Paula (IFD/ICS); Roseth, Benjamin David (IFD/ICS); Mills, Ian Wilfrid (CCB/CCB); Laura Rodriguez Hernandez (IFD/ICS)
▪ Taxonomy:	Research and Dissemination
▪ Operation Supported by the TC:	.
▪ Date of TC Abstract authorization:	29 Feb 2024.
▪ Beneficiary:	Governments of The Bahamas, Barbados, Belize, Guyana, Jamaica, Suriname and Trinidad and Tobago
▪ Executing Agency and contact name:	Inter-American Development Bank
▪ Donors providing funding:	OC Strategic Development Program Window 3 - Transitory Emerging Need for Sustainable Development in the Caribbean(W3B)
▪ IDB Funding Requested:	US$1,000,000.00
▪ Local counterpart funding, if any:	US$0
▪ Disbursement period (which includes Execution period):	36 months, with execution expected over a 30-month period
▪ Required start date:	December 1, 2024
▪ Types of consultants:	Consulting Firms and Individuals
▪ Prepared by Unit:	IFD/ICS-Innovation in Citizen Services Division
▪ Unit of Disbursement Responsibility:	IFD/ICS-Innovation in Citizen Services Division
▪ TC included in Country Strategy (y/n):	Yes
▪ TC included in CPD (y/n):	No
▪ Alignment to the Update to the Institutional Strategy 2024-2030:	Institutional capacity and rule of law

II. Objectives and Justification of the TC

2.1 The objective of this Technical Cooperation (TC) is to support the Governments of beneficiary countries from the Caribbean in strengthening their cybersecurity[1] national

[1] According to the International Telecommunication Union (ITU), cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions,

governance, policy agendas, and in responding to high-impact cybersecurity incidents. The specific objectives of this TC are to provide technical assistance to the Governments in: (i) assessing their current national-level cybersecurity governance and public policy posture; (ii) recommending action plans for their strengthening, with emphasis on opportunities for regional collaboration, coordination and improving economies of scale; (iii) disseminating findings and conducting policy dialogues and (iv) providing immediate technical assistance in cases of high-impact cybersecurity incidents.

2.2 **Justification.** In the aftermath of the COVID-19 crisis, governments throughout Latin America and the Caribbean are continuing to accelerate their economic recovery with increased reliance on the benefits of the digital economy. However, in an effort to quickly engage in the digital economy, the establishment of effect cybersecurity protocols and systems were not prioritized[2]. As a result, regional governments are now confronted by increased vulnerabilities, increasing the salience for protecting cyberspace at the national, sectoral and organization-specific levels.

2.3 An organization in the Caribbean is being attacked an average of 672 times per week. About 3.1% of organizations suffer from a malware infection on a given week, 3.0% from a Botnet infection, and 4.2% from information stealer malware. The cyber threat landscape in Caribbean countries includes, among other threats, ransomware used for extorsion, hacktivism, and threats to the IT supply chain (3rd party risk)[3].

2.4 These underlying cybersecurity vulnerabilities occasionally result in high-profile cybersecurity attacks, affecting all countries. An incomplete sample of high-impact incidents in 2023 may include: In the Bahamas, some of the organizations breached include the registrar general's office, ZNS, and the public treasury[4]. In Barbados, the government shut down its entire IT platform due to a ransomware attack in March 2022[5], and between December 2022 and January 2023, IT systems in Queen Elizabeth Hospital were offline for weeks due to an attack[6]. In Belize, Belize Electricity Limited suffered a data leak[7]. In Guyana, government entities were infected by a previously unknown backdoor placed by a suspected state actor[8]. In Jamaica, the Financial Services Commission suffered from a cyberattack. In Trinidad and Tobago, the Office of The Attorney General and the National Insurance Board were hit by ransomware. And in Suriname, gang hacking and scamming activity was detected online[9], and the press was repeatedly attacked[10].

---

training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets.

2 Minto-Coy, I. D., & Henlin, M. G. G. (2018). The Development of Cybersecurity Policy and Legislative Landscape in Latin America and Caribbean States. In Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications (pp. 286-308). IGI Global.

3 Data provided by Checkpoint Research for the first half of 2013.

4 https://www.thenassauguardian.com/business/thompson-bahamas-not-doing-that-well-at-cybersecurity/article_ac44c6b0-941e-588c-963d-ee84e05dbfca.html

5 https://nationnews-brb.newsmemory.com/publink.php?shareid=130e9f0cf (article no longer available)

6 https://barbadostoday.bb/2023/01/15/qeh-departments-being-reconnected-to-internet-after-cyber-attack/amp/

7 https://www.caribbeantoday.com/sections/news-2/belize-electricity-limited-has-had-its-it-network-hacked

8 https://therecord.media/suspected-china-linked-hackers-target-guyana-government

9 https://csirt.sr/tikkers-bende-actief-als-hackers-en-scammers-op-facebook/

10 https://latamjournalismreview.org/news/suriname-media-owners-complain-of-organized-cyber-attacks/

2.5 These attacks occur in the context of weak governmental capacity to prevent, detect and respond to cyberattacks. While the individual maturity of each of the countries varies according to different maturity evaluations, most of the countries do not have a National Cybersecurity Strategy, the capacity of their governmental cybersecurity incident response teams in extremely limited including up to five professionals, and none have a national cybersecurity agency or a critical infrastructure protection plan.

2.6 Regional governments are committed to change this reality through individual and as well as collaborative efforts: In the Port of Spain Commitment on Digital Integration, Caribbean Ministers with responsibility for ICT and Digital Transformation declared in May 2023 their recognition of the need for joint and focused action on cybersecurity challenges. Specifically, the Ministers agreed to develop a regional Cyber Security Incident Response Team (CSIRT) to coordinate collaboration among national CSIRTs; enhance cybersecurity training, education and awareness to address the skills gap and to promote safe online practices; and to develop a Critical Infrastructure Protection Regional Framework.

2.7 The IDB has responded to the abovementioned cybersecurity challenges with a number of capacities building efforts, including loan operations and specific technical assistance. In The Bahamas, 4549/OC-BH includes specific support for cybersecurity, and the International Telecommunications Union (ITU) is consulting the government in improving its capacity. In Barbados, 4920/OC-BA finances the design of a cybersecurity strategy. In Jamaica, JA-L1093 (in design) focuses exclusively on cybersecurity capacity building, and United States Agency for International Development (USAID) is currently providing assistance to the national cybersecurity authorities. In Trinidad and Tobago ATN/JF-20080-TT focuses exclusively on cybersecurity and 5841/OC-TT includes a significant component supporting cybersecurity investment. In Suriname, ATN/JF-19603-SU is dedicated to providing cybersecurity technical assistance. Other international organizations such as the Organization of American States (OAS) and Caribbean Community (Caricom) also support the region in cybersecurity capacity building; all countries have participated in regional capacity building activities such as the IDB-OAS regional cybersecurity maturity study[11], the IDB's National Cybersecurity Leadership course, and the IDB's Caribbean Cybersecurity Conference held in Nassau, Bahamas in late 2019. The IDB-OAS study found that most of this program's beneficiary countries counted among those with less mature cybersecurity capabilities (compared with other LAC countries), underlining the need for greater efforts in the area. Through its various dimensions and indicators, it has also highlighted specific areas for attention for each country, which will inform this program's activities.

2.8 The IDB is in a unique position to support Caribbean governments' cybersecurity capacity building, given our ongoing investment and technical assistance projects, and proven record leveraging technical support from the most advanced countries in cybersecurity worldwide. For example, the government of Israel has supported capacity in cybersecurity throughout Latin America since 2016 and is currently involved providing access for the region's cybersecurity professionals to the most advanced training, knowledge, expertise and best practices worldwide (ATN/CF-15598-RG, ATN/CF-19154-RG). The contexts of Japan, Korea and Spain also portend meaningful lessons and technical support in state capacity and the

[11] https://publications.iadb.org/en/2020-cybersecurity-report-risks-progress-and-the-way-forward-in-latin-america-and-the-caribbean

co-production of cybersecurity (ATN/JF-20080-TT, ATN/JF-19603-SU, ATN/KR-19795-RG, ATN/FG-16633-RG and ATN/FG-18691-RG).

2.9 **Strategic alignment.** The TC is consistent with the IDB Group Institutional Strategy: Transforming for Scale and Impact (CA-631) and is strategically aligned with the core objective of bolstering sustainable regional growth, and with the focus area of Institutional Capacity, Rule of Law, and Citizen Security by strengthening beneficiary governments' capacity to secure their digital activities, critical operations and the national cyberspace. It is aligned with Window 3B of The Ordinary Capital Strategic Development Program (OC SDP) (GN-2819-14), which is the ONE Caribbean (Partnering for Caribbean Development Framework) (GN-3201-5) program, specifically in the priority area of Citizen Security, and the cross-cutting areas of strengthening technical capabilities and institutional capacity and of digitalization of the public sector. It is expected to contribute to ONE Caribbean results such as improved disaster preparedness and greater access to resilient infrastructure across the region; safer communities through crime prevention; and enhanced investment and productivity. Finally, this TC aligns with the each of the beneficiary country strategies of the Bank with (i) The Bahamas (GN-3198-1 for 2024-28), specifically in the areas of enhancing the capacity of the state, facilitating the use of technologies, disaster risk management, and strengthening public sector governance through digital transformation, among other areas; (ii) Barbados (GN-2953-1 for 2019-2023[12]), specifically in the priority area of public sector efficiency through implementing a public sector digital strategy; (iii) Belize (GN-3086 for 2022-2025), specifically in promoting digital transformation in the government; (iv) Guyana (GN-3187 for 2023-2026), specifically in strengthening institutional capacity through the introduction of technology/information systems to improve efficiency in public services; (v) Jamaica (GN-3138 for 2022-2026), specifically in supporting the modernization of the policy and regulatory framework for cybersecurity; (vi) Suriname (GN-3065 for 2021-2025), specifically in strengthening the digital transformation enabling framework particularly around cybersecurity; and (vii) Trinidad and Tobago (GN-3071 for 2021-2025), specifically in strengthening cybersecurity protection of digital infrastructure.

III. Description of activities/components and budget

3.1 **Component I. Diagnostics, Action Plans and Specialized Consultancies for Public Policy and Governmental Capacity in Cybersecurity (US$250,000).** Under this component, (i) a consultancy project would: assess the current cybersecurity threats, vulnerabilities, governance and public policy posture of each beneficiary country; recommend per-country opportunities and action plans for their strengthening and identify and propose specific opportunities for beneficiary country coordination, collaboration, improving synergies and economies of scale[13]. And (ii) in addition, specialized cybersecurity technical assistance will be provided to beneficiary governments. This assistance will respond to dynamic cybersecurity public policy and capacity building needs of beneficiary governments and will build upon and complement recent similar technical assistance and investment initiatives benefitting

---

12 Extended by GN-2953-3 until May 2025.

13 This single consulting project would conduct bottom-up analysis for each country, based on existing information such as IDB-OAS country cybersecurity maturity evaluations, specific previous consultancy work, and interviews with key authorities. Per country strategic proposals would be made to attend identified gaps, as well as a specific section focused on identifying and designing proposals for multi-country collaboration among beneficiaries.

several of the countries. Two instances of specialized assistance are expected to be financed by this activity.

3.2 **Component II. Cybersecurity Policy Dialogues and Dissemination (US$150,000).** Under this component, beneficiary governments will dialogue to explore opportunities for collaboration, coordination, synergies and economies of scale. The IDB will undertake the following activities: (i) organize two Regional Cybersecurity Policy Dialogue events. The first will inform the diagnostics and action plans created in Component I; and the second will present and discuss its draft results and (ii) report and disseminate the results of the diagnostics, action plans and policy dialogues. International organizations that could potentially contribute or lead regional initiatives such as CARICOM and the Caribbean Telecommunications Union will be invited to the dialogues and workshops.

3.3 **Component III. Immediate Technical Assistance for High-Impact Cyber Incident Response (US$500,000).** This component will pre-contract specialized cybersecurity services to respond and recover from high-impact cybersecurity incidents. In case of cybersecurity incidents severely impacting governmental and other critical functions[14], public sector entities from beneficiary countries could benefit from highly specialized cybersecurity services to complement their in-house abilities in the immediate time frame, until such services can be separately contracted in the short to medium time frame. Such services may include incident response, investigation including causes and effects, negotiation, communication, recovery, vulnerability identification remediation and testing, and similar as needed. Where feasible, professional knowledge transfer in cyber-incident response practices to affected organizations cybersecurity and IT personnel will be included in incident response plans.

3.4 **Project Administration, Travel and Unforeseen Expenses (US$100,000).** This activity will finance a consultant to organize, convene, contract, document, monitor and report the consulting contracts, two international dialogues and dissemination activities planned under this project, as well as monitoring and evaluation, related travel and unforeseen expenses.

3.5 **Expected Results**. The expected result of this TC is the institutional and operational strengthening of the beneficiary governments and critical institutions to reduce the potential impact of cybersecurity incidents. Longer term impact reduction would be achieved through promoting new public policy measures based on consulting activities (Component I activities dialogued and disseminated through Component II activities). Immediate term impact reduction would be achieved through improved[15] rapid cybersecurity incident response services (Component III activities). The direct beneficiaries include governmental and other critical public sector organizations suffering from high impact cyberattacks and government cybersecurity personnel tasked with cybersecurity public policy and incident response.

3.6 **Sustainability**. This project will contribute to strengthening permanent cybersecurity capabilities in beneficiary countries in aspects currently insufficiently developed. Specifically, Component I activities will advise individual governments, creating

---

[14] In this component, critical functions include those required to sustain the lives, health, safety including public safety, environment, economy, rule of law, symbols of the state, fundamental rights and similar important values through essential services like healthcare, energy, transportation, law enforcement, government, the financial system, essential supply chains and others.

[15] Improved in comparison to the counterfactual situation where this technical assistance is not available.

relevant knowledge and workplans which will be informed, discussed and disseminated through Component II. In addition, opportunities for multi-country collaboration will be mapped and brought forward, further benefitting participants with opportunities not previously available. In line with the Port of Spain Commitment on Digital Integration, potential opportunities such as a regional CSIRT and training can create and enhance sustainable incident response capabilities to address currently unmet cybersecurity needs, thus eventually replacing Component III's immediate technical assistance facility.

3.7 **Indicative budget.** This project is funded by OC Strategic Development Program Window 3 - Transitory Emerging Need for Sustainable Development in the Caribbean (W3B). The total amount of funding required for this TC is US$1,000,000, as shown below:

Indicative Budget

Activity/Component	Description	Total IDB Funding US$
Component I. Diagnostics, Action Plans and Specialized Consultancies for Public Policy and Governmental Capacity in Cybersecurity	One document per participating government with findings and recommendations; one document suggesting multinational opportunities for collaboration; two instances of specialized cybersecurity technical assistance for capacity building	250,000
Component II. Cybersecurity Policy Dialogues and dissemination	Two policy dialogues and one technical note of discussions and recommendations	150,000
Component III. Immediate Technical Assistance for High-Impact Cyber Incident Response	Technical assistance provided to recover from four high-impact cybersecurity incidents	500,000
Project Administration, Travel and Unforeseen Expenses		100,000
Total		1,000,000

IV. Executing agency and execution structure

4.1 The Executing Agency will be the Inter-American Development Bank (IDB), through the Innovation in Citizen Services Division (IFD/ICS), in accordance with the guidelines and requirements established in the Technical Cooperation Policy (GN-2470-2) and in the Procedures for the Processing of Technical Cooperation Operations and Related Matters (Annex II of OP-619-4). The TC will be implemented over 36 months, with execution expected over a 30-month period. Written requests for all technical assistance activities will be received from beneficiary countries prior to realizing said activities. Owing to the multi-agency scope of the TC; involvement of state and non-state actors; and recent experience executing cybersecurity reform initiatives throughout the sub-region, IFD/ICS is best equipped to manage this operation and to assure the coordination needed.

4.2 **Procurement**. The activities to be executed under this operation will be included in the Procurement Plan and carried out in accordance with the Bank's established procurement methods, namely: (i) hiring of individual consultants, as established in the regulations AM-650; and (ii) hiring of consulting firms for services of an intellectual nature and the contracting of logistics services and non-consulting services, according to the Corporate Procurement Policy (GN-2303-33) and its associated Guidelines.

4.3 **Intellectual Property**. The knowledge products generated from Bank-executed activities within this technical cooperation will be the property of the Bank and may be made available to the public under a creative commons license. However, at the request of the beneficiaries, in accordance with the provisions of AM-331, the intellectual property of said products may also be licensed through specific contractual commitments that shall be prepared with the advice of the Legal Department.

V. Major issues

5.1 There is a noteworthy risk to effective project implementation, namely orchestrating the participation of all beneficiary countries and assuring all derive benefits from this project's activities, in the context of varying levels of maturity, differing circumstances, and individual technical assistance and loan resources mobilized. Mitigating this risk will involve engaging high-level government officials such as Ministers and Permanent Secretaries in charge of cybersecurity to assure all governments' active participation in project activities. Another risk is the variability of cyber incident characteristics such as timing, scale, type, those affected and similar. This risk will be mitigated by precontracting a number of providers under flexible terms to provide maximal dexterity as incidents occur. In case the volume of incidents handled will be smaller than expected, related Component III resources will become available to enhance the technical assistance provided through Components I and II.

VI. Exceptions to Bank policy

6.1 This operation does not foresee any exceptions to Bank policy.

VII. Environmental and Social Aspects

7.1 This TC will not finance feasibility or pre-feasibility studies of investment projects or associated environmental and social studies; therefore, it does not have applicable requirements of the Bank's Environmental and Social Policy Framework (MPAS).

Required Annexes:

Results Matrix_39685.pdf

Terms of Reference_85514.pdf

Procurement Plan_93408.pdf