TERMS OF REFERENCE - *COMPONENT I ACTIVITY 1*

Caribbean Country and Regional Cybersecurity Posture Assessment

1. Background and Justification

1.1. In 2020, the technical study "Cybersecurity Report: Risks, Progress, and the Way Forward" was developed and published by the Inter-American Development Bank (IDB), in collaboration with the Organization of American States (OAS). This report analyzed the state of preparedness of 32 countries in the region, based on 52 indicators of cybersecurity capability. It constitutes the first significant examination of the level of preparedness of the region against the growing frequency and sophistication of cyber threats and threat actors. According to its findings, the region is in a very incipient state regarding national cybersecurity policies and frameworks. With 20 out of 32 countries without a national cybersecurity strategy, the lack of a clear cybersecurity vision at the national level also hampers countries' involvement in the international cyberspace debate and in the formulation of international norms.

1.2. Further exacerbating this trend, in the aftermath of the COVID-19 crisis, governments throughout Latin America and the Caribbean have taken the decision to continue accelerating 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. 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.

1.3. 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).

1.4. These underlying cybersecurity vulnerabilities occasionally result in high-profile cybersecurity attacks, affecting all countries. As such, these attacks occur in the context of insufficient governmental capacity to prevent, detect and respond to cyberattacks. While the individual maturity of each of the countries varies according to different maturity evaluations, generally 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.

1.5. 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 on May 2023 their recognition of the need for joint and focused action on cybersecurity challenges. Specifically, the Ministers agreed to develop a regional 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.

1.6. The IDB has responded to the abovementioned cybersecurity challenges with a number of capacity building efforts, including loan operations and specific technical assistance. In The Bahamas, BH-L1045 includes specific support for cybersecurity, and the ITU is consulting the government in improving its capacity. In Barbados, BA-L1046 finances the design of a cybersecurity strategy. In Jamaica, JA-L1093 (in design) focuses exclusively on cybersecurity capacity building, and USAID is currently providing assistance to the national cybersecurity authorities. In Trinidad and Tobago TT-T1137 focuses exclusively on cybersecurity and TT-L1061 includes a significant component supporting cybersecurity investment. In Suriname, SU-T1158 is dedicated to providing cybersecurity technical assistance. Other international organizations such as the OAS and 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, the IDB's National Cybersecurity Leadership course, and the IDB's Caribbean Cybersecurity Conference held in Nassau, Bahamas in late 2019.

1.7. The Bank 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 (RG-T2788, RG-T4010). The contexts of Japan, Korea and Spain also portend meaningful lessons and technical support in state capacity and the co-production of cybersecurity (TT-T1137, SU-T1158, RG-T4172, RG-T3024 and RG-T3741).

2. Objectives

2.1. The objective of this contract is to support the strengthening of beneficiary countries' public policy and governmental capacity in cybersecurity by:

- 2.1.1. Assessing the current cybersecurity threats, vulnerabilities, governance and public policy posture of each beneficiary country;
- 2.1.2. Recommending per-country opportunities and action plans for their strengthening;
- 2.1.3. Identifying and proposing specific opportunities for beneficiary country coordination, collaboration, improving synergies and economies of scale;
- 2.1.4. Organizing two Regional Cybersecurity Policy Dialogue meetings to support these objectives.

3. Key Activities

3.1. Assess the current cybersecurity threats, vulnerabilities, governance and public policy posture of each beneficiary country by conducting a 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;

3.2. Formulate per country strategic proposals and action plans required to effectively address the gaps identified in activity 3.1 and improve each beneficiary country's public policy and governmental capacity in cybersecurity;

3.3. Identify and design proposals for multi-country collaboration among beneficiaries in order to improve synergies and economies of scale;

3.4. Present the draft results of activities 3.1, 3.2 and 3.3 for feedback;

3.5. Finalize and submit reports on activities 3.1, 3.2 and 3.3 thus providing professional input to the process of strengthening beneficiary countries' public policy and governmental capacity in cybersecurity. The final reports should incorporate feedback gathered during activity 3.4;

3.6. Organize two Regional Cybersecurity Policy Dialogue events:
- 3.6.1. The first event will inform activities 3.1, 3.2 and 3.3;
- 3.6.2. The second event will present the draft results for feedback and discussion (activity 3.4).

4. Expected Outcome and Deliverables

4.1. Workplan indicating timeline and methodology for the completion of contract activities;
4.2. Draft report on activity 3.1;
4.3. Final report on activity 3.1 after carrying out activity 3.4;
4.4. Draft report on activity 3.2;
4.5. Final report on activity 3.2 after carrying out activity 3.4;
4.6. Draft report on activity 3.3;
4.7. Final report on activity 3.3 after carrying out activity 3.4;
4.8. Events and draft results as described in activities 3.6.1 and 3.6.2.

5. Project Schedule and Milestones

5.1. The work shall be carried out in the span of twelve (12) months from the time of contract signature. The selected firm must present a proposed timeline for completion of the activities within one month of contract signature.

6. Reporting Requirements

6.1. Language: all project activities and communications including draft and final deliverables, presentations, events and similar will be in English;

6.2. Deliverable 4.1: The contents should be up to two pages long;

6.3. Deliverables 4.2 and 4.3, activity 3.1: Should focus on the current situation of the country and

the government's current posture, and identify gaps and unmet needs requiring interventions;

6.4. Deliverables 4.4 and 4.5, activity 3.2: Should lay out the different projects and interventions needed to address the identified gaps and unmet needs, at a level of detail enough to define the essential aspects of each suggestion. This report should be considered a suggested basis for a governmental action plan;

6.5. Deliverables 4.6 and 4.7, activity 3.3: Should highlight opportunities for multi-country collaboration and coordination among beneficiaries, striving to improve synergies and economies of scale in alignment with different governments' needs, capabilities, priorities and action plans;

6.6. Deliverable 4.8:

6.6.1. The Regional Cybersecurity Policy Dialogue events should include presentations of the bottom-up analysis (detailing cybersecurity threats, vulnerabilities, governance and public policy posture) as well as action plans for each country, other relevant presentations and interactive sessions and activities.

6.6.2. The contents of the draft results described in activity 3.6.2 are expected to be between five and seven pages long (in addition to appendixes).

7. Acceptance Criteria

7.1. The Consulting Firm shall maintain regular communication with the point of contact at the IDB in carrying out the activities and developing all deliverables described in this contract. The Consulting Firm shall obtain IDB's approval for the completion of each of the planned activities before associated payments are processed.

7.2. An IDB representative will be copied in all communications between the Consulting Firm and the beneficiary governments.

7.3. All written deliverables will be presented in professional-level English.

7.4. Deliverables will be provided in editable formats (i.e., Microsoft Word, PowerPoint, e-mail etc.), as well as any finalized formats.

8. Other Requirements

8.1. The Consulting Firm and its employees or agents are aware that in discharging their obligations pursuant to this Agreement, they may have access to privileged, confidential and/or proprietary information of the IDB, the Government or of another party in their possession. Under no circumstances, except with the IDB's express written permission, shall Supplier and its employees or its agents copy, reproduce, sell, assign, license, market, transfer, give or otherwise disclose to any person or organization, in any manner or form, now or after the expiration of the Agreement, such Confidential Information or any part thereof. The Consulting Firm must handle, and if needed temporarily retain, all such information under the appropriate safeguards.

8.2. Upon request by the Bank or upon completion of the Work, Supplier will immediately return to the Bank or Government at Supplier's expense all Confidential Information, documents, or data the Supplier accessed through this engagement, and all copies thereof.

9. Supervision

9.1. The IDB shall supervise the execution of the activities and completion of the deliverables indicated in these terms of reference and approve all payments. The points of contact at the IDB for all matters related to this contract will be Ariel Nowersztern, Senior Cybersecurity Specialist (arieln@iadb.org).

10. Payment Schedule

Deliverable	Percentage
Upon contract signature and approval of deliverable 4.1	10%
Approval of deliverable 4.2	10%
Approval of deliverable 4.3	15%
Approval of deliverable 4.4	10%
Approval of deliverable 4.5	15%
Approval of deliverable 4.6	10%
Approval of deliverable 4.7	15%
Approval of deliverable 4.8	15%
TOTAL	100%

TERMS OF REFERENCE – *COMPONENT I ACTIVITY 2*

Cybersecurity Public Policy And Capacity Building

Background and Justification

1.1 In 2020, the technical study "Cybersecurity Report: Risks, Progress, and the Way Forward" was developed and published by the Inter-American Development Bank (IDB), in collaboration with the Organization of American States (OAS). This report analyzed the state of preparedness of 32 countries in the region, based on 52 indicators of cybersecurity capability. It constitutes the first significant examination of the level of preparedness of the region against the growing frequency and sophistication of cyber threats and threat actors. According to its findings, the region is in a very incipient state regarding national cybersecurity policies and frameworks. With 20 out of 32 countries without a national cybersecurity strategy, the lack of a clear cybersecurity vision at the national level also hampers countries' involvement in the international cyberspace debate and in the formulation of international norms.

1.2 Further exacerbating this trend, in the aftermath of the COVID-19 crisis, governments throughout Latin America and the Caribbean have taken the decision to continue accelerating 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. 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.

1.3 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).

1.4 These underlying cybersecurity vulnerabilities occasionally result in high-profile cybersecurity attacks, affecting all countries. As such, these attacks occur in the context of insufficient governmental capacity to prevent, detect and respond to cyberattacks. While the individual maturity of each of the countries varies according to different maturity evaluations, generally 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.

1.5 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 on May 2023 their recognition of the need for joint and focused action on cybersecurity challenges. Specifically, the Ministers agreed to develop a regional 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.

1.6 The IDB has responded to the abovementioned cybersecurity challenges with a number of capacity building efforts, including loan operations and specific technical assistance. In The Bahamas, BH-L1045 includes specific support for cybersecurity, and the ITU is consulting the government in improving its capacity. In Barbados, BA-L1046 finances the design of a cybersecurity strategy. In Jamaica, JA-L1093 (in design) focuses exclusively on cybersecurity capacity building, and USAID is currently providing assistance to the national cybersecurity authorities. In Trinidad and Tobago TT-T1137 focuses exclusively on cybersecurity and TT-L1061 includes a significant component supporting cybersecurity investment. In Suriname, SU-T1158 is dedicated to providing cybersecurity technical assistance. Other international organizations such as the OAS and 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, the IDB's National Cybersecurity Leadership course, and the IDB's Caribbean Cybersecurity Conference held in Nassau, Bahamas in late 2019.

1.7 The Bank 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 (RG-T2788, RG-T4010). The contexts of Japan, Korea and Spain also portend meaningful lessons and technical support in state capacity and the co-production of cybersecurity (TT-T1137, SU-T1158, RG-T4172, RG-T3024 and RG-T3741).

2. Objectives

The objective of this contract is to support COUNTRY's national cybersecurity policy formation by:

i. Assessing the current situation, gaps and challenges in cybersecurity in COUNTRY;
ii. Planning specific improvements to the government's cybersecurity readiness;
iii. Supporting the National Cybersecurity Strategy (NCS) formation.

3. Key Activities

3.1 Assess the current situation, gaps and challenges in cybersecurity in COUNTRY, by:

i. Identifying and mapping the cyberthreats that affect the country's government institutions and critical infrastructure;
ii. Analyzing and identifying gaps in the government's current cybersecurity activities and readiness to handle these threats;

3.2 Plan specific improvements to the government's cybersecurity readiness, by listing and suggesting the scope and expected budget of the main projects and interventions required to effectively address

the gaps identified in activity 3.1.2 and improve the country's cybersecurity readiness, including technological improvements, training, policy changes, a suggested institutional structure, roles and responsibilities and other projects and interventions as required;

3.3 Present the draft results of activities 3.1 and 3.2 for feedback;

3.4 Support the NCS formation process, by:
- 3.4.1 Suggesting a methodology for the NCS formation process;
- 3.4.2 Leading an onsite training workshop on the NCS formation process and methodology;
- 3.4.3 Reporting on the workshop discussion and insights;

3.5 Finalize and submit reports on activities 3.1, 3.2 and 3.4 thus providing professional input to the NCS formation process. The final reports should incorporate feedback gathered during activities 3.3 and 3.4.2.

4 Expected Outcome and Deliverables

4.1 Workplan indicating timeline and methodology for the completion of contract activities;
4.2 Draft report on activity 3.1;
4.3 Final report on activity 3.1 after carrying out activity 3.3;
4.4 Draft report on activity 3.2;
4.5 Final report on activity 3.2 after carrying out activity 3.3;
4.6 Report as a document or presentation on activity 3.4.1;
4.7 Workshop and report as described in activities 3.4.2 and 3.4.3.

5 Project Schedule and Milestones

5.1 The work shall be carried out in the span of twelve (12) months from the time of contract signature. The selected firm must present a proposed timeline for completion of the activities within one month of contract signature.

6 Reporting Requirements

6.1 Language: all project activities and communications including draft and final deliverables, presentations, events and similar will be in English;

6.2 Deliverable 4.1: The contents should be up to two pages long;

6.3 Deliverables 4.2 and 4.3, activity 3.1: Should focus on the current situation of the country and the government's current posture, and identify gaps and unmet needs requiring interventions;

6.4 Deliverables 4.4 and 4.5, activity 3.2: Should lay out the different projects and interventions needed to address the identified gaps and unmet needs, at a limited level of detail enough to define the essential aspects of each suggestion. This report should be considered a suggested basis for a

governmental action plan;

6.5 Deliverables 4.6 and 4.7, activity 3.4:

6.5.1 The workshop should include presentations of the methodology, other relevant presentations and interactive sessions and activities. The workshop should be at least two full days long, in addition to any time spent on activity 3.3;

6.5.2 The contents of the report described in activity 3.4.3 are expected to be between five and seven pages long (in addition to appendixes).

6.6 Onsite visits:

6.6.1 This contract requires at least two team onsite visits: the first for activity 3.1, estimated at five full working days, and the second for activity 3.3, estimated at two to three full working days.

6.6.2 Activities 3.2 and 3.5 are not required to be onsite.

6.6.3 Activity 3.4.2 (workshop) will be done onsite. It is expected to be carried sequentially with activity 3.3, but could be conducted separately as will be agreed in coordination with the IDB and COUNTRY'S National CSIRT.

7 Acceptance Criteria

7.1 The Consulting Firm should comply with the following requirements and qualifications:

7.1.1 The main activity and focus of the Consulting Firm must be on Cybersecurity with a proven record and experience in policy, assessments, and implementation of projects in diverse international settings;

7.1.2 The Consulting Firm must be a for-profit organization;

7.1.3 The Lead Consultant must have at least 10 years of proven and successful experience in Cybersecurity with at least two years of experience in National Cybersecurity Policy.

7.2 The Consulting Firm shall maintain regular communication with the point of contact at the IDB, as well as the representatives at the client unit, the COUNTRY'S National CSIRT, in carrying out the activities and developing all deliverables described in this contract. The consulting firm shall obtain the IDB's approval of each deliverable before associated payments will be processed.

8 Supervision

8.1 The IDB and COUNTRY'S National CSIRT shall supervise execution of the activities and completion of the deliverables indicated in these terms of reference and approve all payments. The point of contact at the IDB for all matters related to this contract will be Ariel Nowersztern, Senior Cybersecurity Specialist (arieln@iadb.org).

9 Payment Schedule

Deliverable	Percentage
Upon contract signature and approval of deliverable 4.1	15%
Approval of deliverable 4.2	10%
Approval of deliverable 4.3	10%
Approval of deliverable 4.4	10%
Approval of deliverable 4.5	10%
Approval of deliverable 4.6	15%
Approval of deliverable 4.7	30%
TOTAL	100%

TERMS OF REFERENCE – *COMPONENT III*

Immediate Technical Assistance For High-Impact Cyber Incident Response

1. Background and Justification

1.1 In 2020, the technical study "Cybersecurity Report: Risks, Progress, and the Way Forward" was developed and published by the Inter-American Development Bank (IDB), in collaboration with the Organization of American States (OAS). This report analyzed the state of preparedness of 32 countries in the region, based on 52 indicators of cybersecurity capability. It constitutes the first significant examination of the level of preparedness of the region against the growing frequency and sophistication of cyber threats and threat actors. According to its findings, the region is in a very incipient state regarding national cybersecurity policies and frameworks. With 20 out of 32 countries without a national cybersecurity strategy, the lack of a clear cybersecurity vision at the national level also hampers countries' involvement in the international cyberspace debate and in the formulation of international norms.

1.2 Further exacerbating this trend, in the aftermath of the COVID-19 crisis, governments throughout Latin America and the Caribbean have taken the decision to continue accelerating 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. 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.

1.3 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).

1.4 These underlying cybersecurity vulnerabilities occasionally result in high-profile cybersecurity attacks, affecting all countries. These attacks occur in the context of insufficient governmental capacity to prevent, detect and respond to cyberattacks. While the individual maturity of each of the countries varies according to different maturity evaluations, generally 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.

1.5 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 on May 2023 their recognition of the need for joint and focused action on cybersecurity challenges. Specifically, the Ministers agreed to develop a regional 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.

1.6 The IDB has responded to the abovementioned cybersecurity challenges with a number of capacity building efforts, including loan operations and specific technical assistance. In The Bahamas, BH-L1045 includes specific support for cybersecurity, and the ITU is consulting the government in improving its capacity. In Barbados, BA-L1046 finances the design of a cybersecurity strategy. In Jamaica, JA-L1093 (in design) focuses exclusively on cybersecurity capacity building, and USAID is currently providing assistance to the national cybersecurity authorities. In Trinidad and Tobago TT-T1137 focuses exclusively on cybersecurity and TT-L1061 includes a significant component supporting cybersecurity investment. In Suriname, SU-T1158 is dedicated to providing cybersecurity technical assistance. Other international organizations such as the OAS and 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, the IDB's National Cybersecurity Leadership course, and the IDB's Caribbean Cybersecurity Conference held in Nassau, Bahamas in late 2019.

1.7 The Bank 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 (RG-T2788, RG-T4010). The contexts of Japan, Korea and Spain also portend meaningful lessons and technical support in state capacity and the co-production of cybersecurity (TT-T1137, SU-T1158, RG-T4172, RG-T3024 and RG-T3741).

2 Objectives

2.1 The objective of this contract is to support specific Public-Sector and Critical organizations affected by cybersecurity incidents in quickly and efficiently responding to these incidents and recovering their systems, to facilitate the resumption of normal services.

3 Key Activities

Consultancy activities may include multiple instances of the following kinds of professional services, as deemed necessary, planned, agreed, and approved in accordance with section 4.1 during contract execution:

3.1 **Recovery:** Assist the organization's IT team in recovering systems and data from backups to resume normal services.

3.2 **Forensics:** Assist the organization's IT team in determining and reporting any aspects related to the attack, such as information accessed, information exfiltrated, timeline and events of the attack.

3.3 **Remediation:** Assist the IT team in testing said systems for attacker presence and removing any persistent threats.

3.4 **Hardening:** Assist the IT team in suggesting secure system designs and/or in implementing recommendations for hardening their systems to prevent recurrent or future attacks, for example patching, network segmentation, two-factor authentication, and other protective measures.

3.5 **Hardening review:** Following the IT systems hardening, the organizations or independent consultants may review and test the recommendations' implementation by the Consulting Firm (realized through activity 3.3), potentially by follow-up calls, technical testing, or ethical hacking methods. The contracted firm will be responsible for attending remaining gaps identified by the review.

3.6 Review and advise regarding security policies, systems design, and contingency plans.

3.7 **Ethical hacking:** Perform ethical hacking services in case these are requested:

- 3.7.1 **Targets:** The Client, the Consulting Firm and the IDB will hold a dialogue to define the target systems and techniques applicable to be tested in the context of any specific request. These may include Client IT Infrastructure, Applications, or both:
  - 3.7.1.1 **Infrastructure:** Conventional attacks on exposed IT Infrastructure with a focus on identifying and exploiting software, configuration, or credential flaws.
  - 3.7.1.2 **Applications:** Testing web and mobile components with a focus on obtaining access to or modifying sensitive information, or on building client-side attacks that could be used in other testing techniques (e.g., phishing).
- 3.7.2 **Tools:** The penetration testing will be carried out using both automated and manual tools.
- 3.7.3 **Methods:** The penetration testing will usually be done using "Gray Box" methods; In some cases, "White Box" or "Black Box" methods may be selected in mutual agreement.

3.8 **Monitoring:** Implement market-leading monitoring solution(s) on the IT systems, of kinds to be specified and agreed during contract execution, including Endpoint Detection and Response (EDR), and Extended Detection and Response (XDR), in order to detect possible ongoing, recurrent, or future attacks. Said monitoring is required to bring systems back online and resume normal services. The contracted firm will provide the monitoring solutions and support the IT team in reviewing and handling findings detected by these solutions, for an interim period the duration of which will be agreed and approved during contract execution in accordance with section 4.1. During that period, monitoring solutions would be procured and implemented for the long term directly by the Client.

3.9 Any other professional cybersecurity services, to be agreed.

4 Contract Execution

4.1 **Planning and approval:** The Consulting Firm will develop written plan(s) to realize instances of abovementioned activities, of the types denoted in 3.1 through 3.9, as will be required during contract execution. Each plan will specify aspects such as the activities to be carried out, responsibilities of the Consulting Firm and the Client organization, methodologies and tools used, specific systems in the activity's scope, the time schedule and the number of service hours charged to carry out each activity. Said plan(s) must be approved in writing by the contract supervisors prior to implementation.

4.2 **Implementation:** The Consulting Firm will perform the services according to the approved plan(s), prioritizing speed and efficiency of execution while realizing the determined objectives.

4.3 **Reporting:** The Consulting Firm will report in writing to the IDB and the Client teams regarding the implementation of the abovementioned plans and activities, as well as on findings and recommendations to correct any deficiencies. The report shall include: an executive summary, the methodology used, activities carried out, findings grouped by levels of risk, screenshots documenting activities and findings, specific and general recommendations.

4.4 **Coordination:** The Consulting Firm will carry out the services in coordination –as relevant– with the affected government units, their IT teams, cybersecurity government agencies, and other consultants engaged by the government or by the IDB, each performing their respective roles and tasks.

4.5 **Status meetings:** Regular meetings will be held to follow-up on the execution of project activities, including representatives of the Consulting Firm, the Government, and the IDB. They are expected to be held on an as-needed frequency, initially daily or bi-weekly, but in any case, at least once a week.

4.6 **Personnel:** The consulting firm would present the specific professionals who would take part in any of the activities to the Government and to the IDB, detailing their experience and credentials, and obtain approval for their participation prior to involving each and any specific professional in said activities.

5 Expected Outcome and Deliverables

5.1 Up to 1,500 (one thousand five hundred) hours of cybersecurity professional services performed through activities 3.1 through 3.9 as defined and approved.

5.1.1 This contract may be finalized or expire regardless of the number of professional service hours consumed, whether any, some or all of the service hours were approved or delivered.

5.2 Specific deliverables will include:

5.2.1 Short form written plan(s), delivered through activity 4.1;

5.2.2 Detailed reports, delivered through activity 4.3.

6 Project Schedule and Milestones

6.1 The totality of services performed shall be carried out within the approved budget and timeframe for the contract. Specific activities therein, including reporting (activity 4.3), shall be executed and reported within the number of service hours and timeframes established by the approved plans (activity 4.1).

6.2 To meet the project schedule, full and timely availability of Client IT team, independent consultants and IDB points of contact are confirmed.

7 Acceptance Criteria

7.1 The Consulting Firm shall maintain regular communication with the point of contact at the IDB and the Client teams, in carrying out the activities and developing all deliverables described in this contract. The Consulting Firm shall obtain IDB's approval for the completion of each of the planned activities before associated payments are processed.

7.2 An IDB representative will be copied in all communications between the Consulting Firm and the Client.

7.3 All written deliverables will be presented in professional-level English.

7.4 Deliverables will be provided in editable formats (i.e., Microsoft Word, PowerPoint, e-mail etc.), as well as any finalized formats.

8 Other Requirements

8.1 The Consulting Firm and its employees or agents are aware that in discharging their obligations pursuant to this Agreement, they may have access to privileged, confidential and/or proprietary information of the IDB, the Government or of another party in their possession. Under no circumstances, except with the IDB's express written permission, shall Supplier and its employees or its agents copy, reproduce, sell, assign, license, market, transfer, give or otherwise disclose to any person or organization, in any manner or form, now or after the expiration of the Agreement, such Confidential Information or any part thereof. The Consulting Firm must handle, and if needed temporarily retain, all such information under the appropriate safeguards.

8.2 Upon request by the Bank or upon completion of the Work, Supplier will immediately return to the Bank or Government at Supplier's expense all Confidential Information, documents, or data the Supplier accessed through this engagement, and all copies thereof.

9 Supervision and Reporting

9.1 The IDB shall supervise the execution of the activities and completion of the deliverables indicated in these terms of reference and approve all payments. The points of contact at the IDB for all matters related to this contract will be Ariel Nowersztern, Senior Cybersecurity Specialist (arieln@iadb.org).

10 Payment Schedule

Deliverable	Percentage
As per agreed number of service hours per each approved plan, on approval of deliverables 5.1 and 5.2 per approved plan, up to a total of 1,600 service hours.	Up to 100%
TOTAL	100%

Cybersecurity Policy and Incident Response Project Administration Consultant

Post of duty: Washington DC

The IDB Group is a community of diverse, versatile, and passionate people who come together on a journey to improve lives in Latin America and the Caribbean. Our people find purpose and do what they love in an inclusive, collaborative, agile, and rewarding environment.

About this position

We are looking for a methodical, resourceful and process-oriented Cybersecurity Project Administration Consultant. As Project Administration Consultant, you will organize, convene, contract, document, monitor and report the consulting contracts, two international dialogues and dissemination activities, as well as cybersecurity incident response activities, planned under our regional project aimed at Strengthening Cybersecurity Policy and Incident Response in the Caribbean.

You will work in the Cybersecurity Team of the Data and Digital Government Cluster, part of the Innovation in Citizen Services (ICS) Division of the Institutions for Development (IFD) department of the IDB. This team is responsible for the coordination of activities to strengthen cybersecurity, withing the institutional capacity of the state to deliver better services to citizens using digital solutions and innovation and to support to the modernization of public management.

What you'll do:

- Organize, convene, help contract, document, monitor and report the consulting contracts, international dialogues, dissemination and incident response activities.

What you'll need

- **Education:** Bachelor's degree (or equivalent advanced degree) in Cybersecurity, Information Technology, Public Management, Public Policy, International Development, or other fields relevant to the responsibilities of the role.
- **Experience:** At least 2 years of professional experience in technology or public-sector project management.
- **Languages:** Proficiency in English and one of the other Bank official languages (Spanish, French or Portuguese) is required.

Key skills:

- Learn continuously.
- Collaborate and share knowledge.
- Focus on clients.
- Communicate and influence.
- Innovate and try new things.

Requirements:

- **Citizenship:** You are a citizen of one of our 48-member countries.
- **Consanguinity**: You have no family members (up to the fourth degree of consanguinity and second degree of affinity, including spouse) working at the IDB, IDB Invest, or IDB Lab.

Type of contract and duration:

- **Type of contract:** International Consultant Part-Time.
- **Length of contract:** 30 months.
- **Work Location:** On site.

What we offer

The IDB group provides benefits that respond to the different needs and moments of an employee's life. These benefits include:

- A **competitive compensation** packages.
- **Leaves and vacations**: 2 days per month of contract + gender- neutral parental leave.
- **Health Insurance**: the IDB Group provides a monthly allowance for the purchase of health insurance.
- **Savings plan**: The IDB Group cares about your future, depending on the length of the contract, you will receive a monthly savings plan allowance.
- We offer assistance with **relocation and visa applications** for you and your family when it applies.
- **Hybrid** and **flexible** work schedules.
- **Development support:** We offer learning opportunities to boost your professional profile such as seminars, 1:1 professional counseling, and much more.
- **Health and wellbeing:** Access to our Health Services Center which provides preventive care and health education for all employees.
- **Other perks:** Lactation Room, Daycare Center, Gym, Bike Racks, Parking, and others.

Consultant Part-Time

- A **competitive compensation** packages.
- A flexible way of working. You will be evaluated by deliverable.

Our culture

At the IDB Group we work so everyone brings their best and authentic selves to work, willing to try new approaches without fear, and where they are accountable and rewarded for their actions.

Diversity, Equity, Inclusion and Belonging (DEIB) are at the center of our organization. We celebrate all dimensions of diversity and encourage women, LGBTQ+ people, persons with disabilities, Afro-descendants, and Indigenous people to apply.

We will ensure that individuals with disabilities are provided reasonable accommodation to participate in the job interview process. If you are a qualified candidate with a disability, please e-mail us at diversity@iadb.org to request reasonable accommodation to complete this application.

Our Human Resources Team reviews carefully every application.

About the IDB Group

The IDB Group, composed of the Inter-American Development Bank (IDB), IDB Invest, and the IDB Lab offers flexible financing solutions to its member countries to finance economic and social development through lending and grants to public and private entities in Latin America and the Caribbean.

About IDB

We work to improve lives in Latin America and the Caribbean. Through financial and technical support for countries working to reduce poverty and inequality, we help improve health and education and advance infrastructure. Our aim is to achieve development in a sustainable, climate-friendly way. With a history dating back to 1959, today we are the leading source of development financing for Latin America and the Caribbean. We provide loans, grants, and technical assistance; and we conduct extensive research. We maintain a strong commitment to achieving measurable results and the highest standards of integrity, transparency, and accountability.

Follow us:

https://www.linkedin.com/company/inter-american-development-bank/

https://www.facebook.com/IADB.org

https://twitter.com/the_IDB