IDB Inter-American Development Bank

REQUEST FOR EXPRESSIONS OF INTEREST
CONSULTING SERVICES

Selection # as assigned by e-Tool: RG-T2788-P006
Selection Method: Simplified Competitive Selection (SCS)
Country: Ecuador
Sector: IFD/ICS
Funding – TC #: ATN/CF-15598-RG
Project #: RG-T2788
TC name: Improving human resources capacity in cybersecurity
Description of Services: Assessment of Ecuador's Cybersecurity Readiness, improvement planning and support in formulating the National Cybersecurity Strategy

Link to TC document: https://www.iadb.org/en/project/RG-T2788

The Inter-American Development Bank (IDB) is executing the above-mentioned operation. For this operation, the IDB intends to contract consulting services described in this Request for Expressions of Interest. Expressions of interest must be delivered using the IDB Portal for Bank Executed Operations (http://beo-procurement.iadb.org/home) by: September 12, 2018, 5:00 P.M. (Washington D.C. Time).

The consulting services ("the Services") include an assessment the current situation, gaps and challenges on cybersecurity in Ecuador; Planning specific improvements to the government's cybersecurity readiness; and supporting the National Cybersecurity Strategy (NCS) formation. The work shall be carried out in the span of six (6) 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.

Eligible consulting firms will be selected in accordance with the procedures set out in the Inter-American Development Bank: *Policy for the Selection and Contracting of Consulting firms for Bank-executed Operational Work* - GN-2765-1. All eligible consulting firms, as defined in the Policy may express an interest. If the Consulting Firm is presented in a Consortium, it will designate one of them as a representative, and the latter will be responsible for the communications, the registration in the portal and for submitting the corresponding documents.

The IDB now invites eligible consulting firms to indicate their interest in providing the services described below in the draft summary of the intended Terms of Reference for the assignment. Interested consulting firms must provide information establishing that they are qualified to perform the Services (brochures, description of similar assignments, experience in similar conditions, availability of appropriate skills among staff, etc.). Eligible consulting firms may associate in a form of a Joint Venture or a sub-consultancy agreement to enhance their qualifications. Such association or Joint Venture shall appoint one of the firms as the representative.

Interested eligible consulting firms may obtain further information during office hours, 09:00 AM to 05:00 PM, (Washington D.C. Time) by sending an email to: Ariel Nowersztern (arieln@iadb.org), Cybersecurity

Specialist, or Darío Kagelmacher (dariok@iadb.org), e-Government and Cybersecurity Consultant.

Inter-American Development Bank
Division: Innovation in Citizen Services Division (IFD/ICS).
Attn: Miguel Porrúa, e-Government Lead Specialist

1300 New York Ave, NW, Washington DC 20577, USA
Tel: +1 202 312-4102
E-mail: mporrua@iadb.org
Web site: www.iadb.org

Assessment of Ecuador's Cybersecurity Readiness, improvement planning and support in formulating the National Cybersecurity Strategy

Draft Summary of Terms of Reference

1. Background and Justification

1.1 A recent report by the IDB on broadband deployment in Latin America and the Caribbean[1] points out the vital role of broadband connectivity and access -and particularly the new communications technologies, applications and services enabled by high-bandwidth networks -in fostering economic, political and social progress. One of the recommendations contained in the report to ensure wider deployment and adoption of broadband in the region is to adapt legal and regulatory frameworks to create greater certainty for users, be they governments, enterprises or consumers.

1.2 The range of devices and individuals connected is shaping a new ecosystem of actors and elements that make connectivity possible. The elements of the ecosystem and the use of the Internet are determining a new concept in the Information and Communications Technology (ICT) arena that is the cyberspace. The cyberspace truly represents the way in which people, companies, governments and machines communicate with each other and carry out transactions. All of them have two common nexuses: (i) network connectivity, and (ii) exchange of information by means of a remote access, which play a key role in facilitating the externalities of the transactions. This new ecosystem has seen the emergence of novel specific harms such as information robbery, cyber terrorist attacks or cyber espionage.

1.3 In January 2012, the World Economic Forum launched the initiative "Partnering for Cyber Resilience". To protect the world from cyber-attacks, the document states that "countries need to set up initiatives for a comprehensive management of cyber-risks."[2] Similarly, the International Telecommunications Union launched the Global Cyber Security Agenda (GCA), which is a framework for international cooperation aimed at enhancing confidence and security in the information society[3]. According to the World Economic Forum, the lack of legal frameworks and mechanisms for international cooperation, disparities in cybercrime and privacy laws, differences in rules regarding extradition, legal procedures and evidence access and handling, as well as the inability to provide assistance to investigate and prosecute cyber criminals remain critical challenges to combat cyber-crime.

1.4 In 2016, the technical study "Cybersecurity Report- Are we ready in Latin America and the Caribbean?" was developed and published by the IDB, in collaboration with the OAS. This report analyzed the state of

---

1 Bridging Gaps, Building Opportunity: Broadband as a Catalyst of Economic Growth and Social Progress in Latin America and the Caribbean: A View from the Industry. Marw, 2012

2 http://www. weforum.org/issues/partnering-cyber-resilience-pcr. June 2012

3 http://www.itu.intlcybersecurity/

preparedness of 32 countries in the region, based on 49 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 generally in a very incipient state regarding national cybersecurity policies and frameworks. With 24 out of 32 countries without a national cyber security 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. Additionally, policymakers in the region lack a holistic understanding of cybersecurity, which may generate flawed policies and legal frameworks in relation to technological issues. However, the starting point towards a solution is having a detailed knowledge of the shortcomings and using this information to define a concrete strategy for action.

1.5 The increasing use of ICT in Ecuador helps increase economic and social activities, but at the same time introduces inherent uncertainties and cybersecurity risks which should be constantly managed. Failing to do that might result in risks materializing and cyber-attacks succeeding, causing unwanted economic and social effects in the country and damaging citizens' safety and their trust in ICT.

1.6 In light of this worldwide movement to raise awareness on the importance of proactive Cyber Defense and in accordance with the IDB's commitment to safeguarding the interests of Latin America and the Caribbean Region (LAC), and with support from the Government of Israel, the IDB approved in 2016 the technical cooperation "Improving Human Resources Capacity in Cybersecurity" (RG-T788; ATN/CF-15598-RG), whose aim is to assist beneficiary countries to strengthen the capacity of the institutions responsible for cybersecurity, by providing government officials and policymakers access to training and lessons learned from the most advanced experiences worldwide.

1.7 Israel is considered one of the most advanced countries worldwide in cybersecurity. The country has more than 300 private firms specialized in the area, and most of the large cybersecurity companies have established research and development centers in Israel. The National Cyber Directorate operates under the umbrella of the Prime Minister and is responsible for the implementation of Israel's national cybersecurity strategy. Israel's advanced expertise can be a valuable source of experience for most of LAC countries that are taking initial steps to set up national cybersecurity policies and initiatives.

2. Objectives

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

2.1.1. Assess the current situation, gaps and challenges in cybersecurity in Ecuador;

2.1.2. Planning specific improvements to the government's cybersecurity readiness;

2.1.3. Supporting the National Cybersecurity Strategy (NCS) formation.

3. Key Activities

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

3.1.1. Identifying and mapping the cyberthreats that affect the country's government institutions and critical infrastructure, by collecting and analyzing open source intelligence data and carrying out interviews with relevant stakeholders;

3.1.2. Analyzing and identifying gaps in the government's current cybersecurity activities and readiness to handle these threats, by onsite visits and interviews;

3.2. Plan specific improvements to the government's cybersecurity readiness, by:

3.2.1. 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;

3.2.2. Planning a Security Operations Center project for government systems (gSOC);

3.3. Present the draft results of activities 3.1 and 3.2 for feedback. The presentations should be done onsite;

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 3.2.1;
4.5. Final report on activity 3.2.1 after carrying out activity 3.3;
4.6. Draft report on activity 3.2.2;
4.7. Final report on activity 3.2.2 after carrying out activity 3.3;
4.8. Report as a document or presentation on activity 3.4.1;
4.9. 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 six (6) 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: Drafts, deliverables, and final products must in Spanish (required) and in English (highly desired).
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 3.2.1: 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 3.2.2: Should design the objectives, establishment process and budget, technology, organization, services, and other relevant aspects of establishing a gSOC, at a limited level of detail to serve as a roadmap for the establishing team;

6.6. Deliverables 4.8 and 4.9, activity 3.4:
6.6.1. 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;
6.6.2. 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).

6.7. Onsite visits

6.7.1. 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.

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

6.7.3. 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.

7. Acceptance Criteria

7.1. The Consulting firm should comply with the following requirements and qualifications;

7.11. 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;

7.12. The Consulting firm must be a for-profit organization;

7.13. 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 Strategy;

7.14. At least one Consultant of the team must have proven experience in the design and/or implementation of a National gSOC or similar;

7.15. At least one member of the team must have proven experience in Latin America and the Caribbean and/or is fluent or native in Spanish.

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, 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.