

**CYBER SECURITY: SETTING THE GROUND FOR A
SECURE CYBER-ENVIRONMENT**

RG-T2380	US\$500,000	BBD
RG-T2408	US\$500,000	CSF

CERTIFICATION

I hereby certify that these operations were approved for financing under the Broadband Special Program (BBD) and the Citizen Security Fund (CSF) through a communication sent by Ana Paula Sánchez (ORP/GCM) on September 27, 2013 on behalf of Sergio Zwi and Claudia Ogliastro.

Also, I certify that resources from the BBD are available up to US\$500,000 and US\$500,000 from the CSF in order to finance the activities described and budgeted in this document. This certification reserves resources for the referenced project for a period of four (4) calendar months counted from the date of eligibility. If the project is not approved by the IDB within that period, the reserve of resources will be cancelled, except in the case a new certification is granted. The commitment and disbursement of these resources shall be made only by the Bank in US dollars. The same currency shall be used to stipulate the remuneration and payments to consultants, except in the case of local consultants working in their own borrowing member country who shall have their remuneration defined and paid in the currency of such country. No resources of the Fund shall be made available to cover amounts greater than the amount certified herein above for the implementation of this operation. Amounts greater than the certified amount may arise from commitments on contracts denominated in a currency other than the Fund currency, resulting in currency exchange rate differences, for which the Fund is not at risk.



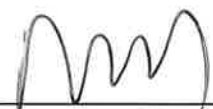
Sonia M. Rivera
Chief
Grants and Co-Financing Management Unit
ORP/GCM

11/13/2013

Date

APPROVAL

Approved by :



Ana María Rodríguez-Ortiz
Sector Manager
Institutions for Development Sector
IFD/IFD

11/22/2013

Date

AP
11/12/2013

REGIONAL TECHNICAL COOPERATION DOCUMENT (TC-DOCUMENT)

I. BASIC INFORMATION

Country:	Regional
TC Name:	Cyber Security: Setting the ground for a secure cyber-environment
TC Number:	RG-T2380/RG-T2408
Team Leader/Members:	Miguel Porrua, Team Leader (IFD/ICS); Antonio García Zaballos (IFD/ICS); Nathalie Alvarado (IFD/ICS); Felix Gonzalez (IFD/ICS); Ricardo Lesperance (IFD/ICS); Alejandro Pareja (IFD/ICS); Nathalia Foditsch (IFD/ICS); Jiyouon Son (IFD/ICS); Javier Bedoya (LEG/SGO); and Cecilia Bernedo (IFD/ICS).
TC Taxonomy:	Research and Dissemination (RD)
Date of TC Abstract authorization:	June, 2013
Beneficiary	Latin America and the Caribbean Region (LAC)
Executing Agency and contact name:	Institutional Capacity of the State Division (IFD/ICS)
Donors providing funding:	Broadband Special Program and Citizen Security Special Program (CSI)
Financing plan:	IDB: Broadband Special Program (RG-T2380): US\$ 500,000 Citizen Security Fund (RG-T2408): US\$ 500,000
Local counterpart:	Local: US\$ 0 Total: <u>US\$1,000,000</u>
Execution period:	36 months
Required start date:	August, 2013
Types of consultants:	Individual Consultants, Consulting firm
Prepared by Unit and UDR:	IFD/ICS
TC Included in Country Strategy:	N/A
TC included in CPD:	N/A

GCI-9 Sector Priority: The current Sector Strategy: “Institutions for Growth and Social Welfare” identifies improving innovation and productivity as a major area where the Bank can help the region overcome the challenges that hinder growth and social welfare. The IDB will work towards strengthening institutions, specifically recognizing the need to improve policies and governmental action in the Information and communication Technology (ICT) sector (5.21 of the referenced Sector Strategy). Consistent with the Strategy, the Bank has approved a Broadband Special Program to accelerate the penetration rate and usage of broadband services in the Region (GN-2704). Citizen security is one of the main areas of the Strategy for institutions for growth and social welfare (IDB Document GN-2587-2). Finally, it was identified as a priority area that contributes to the objectives of the Bank’s ninth capital increase, GCI-9 (Document of the Board of Directors AB-2764). It is further noted that the current “Sector Strategy to Support Competitive Global and Regional Integration” identifies the reduction of the digital divide as one of the Bank’s priorities to promote integration.

II. OBJECTIVE AND JUSTIFICATION

- 2.1 **Background and justification:** A recent report by the Bank on broadband deployment in Latin America and the Caribbean¹ 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.
- 2.2 This panorama of devices and individuals connected is shaping a new ecosystem of players 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

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. Marzo, 2012. <http://www.iadb.org/en/publications/>

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.

- 2.3 The World Economic Forum launched the initiative “Partnering for Cyber Resilience” in January 2012. 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 society³. 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), two complementary initiatives: the Broadband Special Program and the Citizen Security Program have joined forces and established a partnership to co-finance a Technical Cooperation that will begin to explore ways by which the LAC Region can approach and address this very critical and timely issue.
- 2.4 This TC is eligible for funding under the Citizen Security Special Program because its objective is in alignment with one of the pillars of the Citizen Security Initiative which is Information and Analysis on Crime and Violence. The lack of quality data and information to support empirical analyses and diagnostic assessments that make it possible to target public policies more effectively has long been a major obstacle to more effective institutional management of citizen security in LAC. In this knowledge society where much of a country’s daily activities both in the public and private sectors heavily depend on the ICT infrastructure, the security of the citizens in the region has never been more precarious. In accordance with the objectives of the Citizen Security Initiative, this Technical Cooperation will gather valuable information which will first allow the IDB and its member countries to better understand the challenges and potential threats that emanate from the use of new technologies, second demonstrate how a country’s inexpert Cyber Defense can negatively affect its economic outlook, and finally through best practices analyses, this TC will provide the authorities in LAC with information and best practices that can guide their decision-making process in this field and ultimately enable them to better protect the interests of their citizens.
- 2.5 **Objectives.** The ultimate objective of the project is to assist beneficiary countries⁴ in the design of national Cyber Security strategies according to the most recognized international standards thereby strengthening citizen security. An improved legal and regulatory framework (harmonized regionally and compliant with international standards) as well as more updated and shared cyber security information are expected to foster interaction and transaction among the different stakeholders (government, civil society, business community and academia), thus promoting more efficient public and private service delivery to individuals and businesses.
- 2.6 To achieve that goal, the TC has three strategic objectives aligned with the cyber security cycle (prevention, detection and reaction): (i) prevent cyber-attacks; (ii) reduce national

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

³ <http://www.itu.int/cybersecurity/>.

⁴ This TC will focus on all Latin American and Caribbean countries that are members of the IDB.

vulnerabilities to cyber-attacks; and (iii) minimize damage and recovery time from cyber-attacks that occur. In addition, the Bank will assist the selected countries to define strategies that protect critical infrastructure and information. In pursuing those three objectives, the TC will place strong emphasis in identifying and addressing the new threats to the safety of the individual citizen emerging from the cyber space such as identity theft, hacking of bank accounts, virtual kidnapping and cyber bullying, among others.

- 2.7 A key aspect of a sound Cyber Security strategy will be the modernization of the legal and regulatory framework, as indicated by the World Economic Forum⁵. According to WEF, 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; and the inability to provide assistance to investigate and prosecute cyber criminals remain critical challenges to combat cyber-crime. To support the efforts in this area, a model legal and regulatory framework for cyber security will be defined by analyzing the lessons learned from countries that have taken the lead in this area such as USA, Israel, South Korea and the EU members. In addition to the lessons learned from the most advanced countries, a necessary multi-stakeholder approach will require the collaboration with leading IT companies from the telecommunications, software, hardware and consulting fields.
- 2.8 The role of the Bank to accompany countries in their cyber security efforts must be expanded. First, the Bank should help countries conduct an assessment of the current status of cyber security and facilitate a regional exchange based on the findings of this assessment. Second, and based on that regional exchange of experiences and information, the Bank should consider contributing financially and technically to help countries define and implement their comprehensive cyber security strategies so that the gap is bridged.

III. DESCRIPTION OF ACTIVITIES

- 3.1 This operation will have three components: (i) knowledge generation and dissemination; (ii) regional exchange; and (iii) working groups for institutional capacity building.
- 3.2 **Component 1 – Knowledge Generation and Dissemination.** The objective of this component is to determine the status of cyber security in Latin America and the Caribbean by identifying the progress made by each country towards a sound cyber security strategy, the main actors and the needs in each of the countries.
- 3.3 **Activity 1 – International Best Practices.** This activity will document the experiences of the four most recognized countries in *cyber security* worldwide (USA, Israel, South Korea and the EU country members) in terms of capacity building and awareness, regulation and legal framework, policies, governance model–Computer Emergency Response Team (CERTs) –and protection of critical infrastructure (also by means of deployment of cyber infrastructure). This analysis will provide a detailed description of lessons learned that may be applicable to the LAC Region.
- 3.4 **Activity 2 – Diagnosis of Cyber Security in Latin America and the Caribbean.** Through a structured survey, a cyber-security profile of the four sub-regions where the Bank is working will be elaborated including main actors, most critical threats, legal and regulatory framework, policies and initiatives in place, as well as human resource capacity. The document will include recommendations to design cyber-security policies, laws and regulations that tackle the main risks and threats identified. For the diagnosis, a total of

⁵ <http://www.weforum.org/reports/risk-and-responsibility-hyperconnected-world-pathways-global-cyber-resilience>. June 2012.

eight countries will be selected: two from the Caribbean Region, two from the Central American Region, two from the Andean Region and two from the Southern Cone. To select the countries, a call for volunteer countries willing to make the necessary effort will be launched. Given the valuable free expert advice that participating countries will receive, more than the planned two countries per region are expected to volunteer. The two spots per region will be allocated on a first-come-first-serve basis. The survey will be undertaken by conducting on-site structured interviews with cyber security authorities, civil society organizations, academics and businesspeople. The study will be structured based on the five-action pillars defined as key elements for a holistic cyber security plan by the IDB in the document, “From cyber security to cyber-crime: A framework for analysis and implementation”⁶. These pillars are: (i) capacity building and awareness; (ii) regulation and legal framework; (iii) policies; (iv) governance model/CERT; and (v) infrastructure (software and hardware). Special emphasis will be placed in identifying the main attacks suffered by each country and their economic impact.

- 3.5 **Activity 3 – Gap Analysis between the LAC Region and the Leading Countries in Cyber Security.** The study will include a gap analysis that will showcase where LAC countries stand when compared with the more advanced countries in the area of cyber security. In addition, the analysis will identify the minimum standards that any national cyber security strategy should meet in order to protect its citizens from the most common cyber-threats. This gap analysis will be a valuable tool to guide the design of cyber security efforts in the Region. As in the case of the cyber security diagnosis, the survey to conduct the gap analysis will be structured based on the five-action pillars for cyber security planning indicated above. The survey will cover all LAC countries and will be done through a comprehensive online questionnaire that will capture the opinion of relevant stakeholders: government authorities responsible for cyber security, heads of business chambers and associations, recognized academics and researchers, and leaders of civil society organizations active in citizen security or cyber security.
- 3.6 **Activity 4 – Experts Roundtable.** The product resulting from Activity 3 will be analyzed by a group of recognized experts representing the main cyber security stakeholders (government, companies, academia, NGOs) along with IDB experts in order to identify potential areas of action and the value-added that the IDB can offer. This activity will take place at the IDB headquarters and will gather a very limited number of well-known professionals with the aim of providing the IDB with the necessary business intelligence prior to conversations with the Region’s cyber security authorities.
- 3.7 **Activity 5 – Dissemination.** The documents produced under activities 1, 2 and 3, will be edited and published both physically and digitally to facilitate their dissemination not just among the different participants of the activities planned, but also among the cyber security community of Latin American and the Caribbean. These documents will be made available at the online spaces of the Broadband and Citizen Security Initiatives and will be promoted at events organized by both initiatives. In addition, an online platform to facilitate knowledge exchange and collaboration will be launched thereby facilitating the dissemination of all knowledge products generated by this technical cooperation.
- 3.8 **Component 2 – Regional Exchange on Cyber Security Policies.** The knowledge generated in Component 1 of this project will be the foundation of the discussions with the cyber security authorities and the main cyber security stakeholders of the Region.

⁶ Written by Antonio García-Zaballos and Félix González. See Technical Note [IDBDocs#38133436](#).

- 3.9 **Activity 1 – First Regional Exchange on Cyber Security Policies.** This initial workshop will be attended by cyber security authorities, companies, academics, representatives from organized civil society, international experts and relevant international organizations. During this first workshop, the Regional Diagnosis Report, the International Experiences document and the Gap Analysis will be used as the triggers of a multi-stakeholder dialogue aimed at defining the main components of a reliable national cyber security strategy. Discussions held during this Regional Exchange will be structured around the five pillars of a comprehensive cyber security strategy as indicated previously. This will allow for the identification of those areas where the Latin American and Caribbean countries require specific support. This Regional Dialogue will also invite those international organizations that are active in the field of cyber security such as the Organization of American States (OAS), World Economic Forum (WEF), Organization for Economic Cooperation and Development (OECD), International Telecommunication Union (ITU), United Nations Conference on Trade and Development (UNCTAD) and others to present their respective initiatives in order to identify potential synergies and to coordinate efforts.
- 3.10 **Activity 2 – Second Regional Exchange on Cyber Security Policies.** This Second Regional Exchange will be used as an institutional space to monitor the progress towards a more secure Latin American and Caribbean cyberspace as well as strengthen regional coordination and cooperation mechanisms. As was the case in the First Regional Exchange, it will be a multi-stakeholder meeting with the participation of international experts and organizations. The topics for this second regional exchange will be decided based on the discussions held during the first regional exchange and the interests of the Latin American and Caribbean cyber security authorities.
- 3.11 In both regional events the Bank will cover participation costs (plane ticket and per-diem) for one representative per country. This representative will ideally be the highest cyber security authority as per the indication of the corresponding government. Depending on the capacity to add financial sponsors, the Bank will seek to include participation of representatives from the civil society and academic fields, at a minimum of one per Bank region. Other representatives of the private sector, academicians, international organizations and civil society organizations involved in cyber security initiatives will be invited to attend at their own expense.
- 3.12 **Component 3 – Thematic Working Groups.** After each of the two Regional Exchanges, two key topics will be defined as critical to advance the cyber security agenda (such as capacity building and awareness, regulation and legal framework, policies, governance model and protection of critical infrastructure, including deployment of infrastructure). A working group on each of the topics will be set up with the leadership of a recognized expert. Each group will be comprised of representatives of interested countries and will be allocated resources to conduct specific research and training in the area of focus. One group will focus on the new threats to the citizen security arising from the cyber space and what both governments and citizens can do to protect the later. In alignment with the Citizen Security Initiative, this thematic working group will work on three dimensions of the topic: (i) information generation, dissemination and analysis; (ii) policy generation and management; and (iii) regional dialogue and horizontal cooperation.
- 3.13 Each Thematic Working Group will undertake onsite and online workshops and develop specific research concentrated on the target topic. These Groups will include international experts from those countries with the most advanced knowledge in the

topic and produce a document to share the knowledge with the Region and to present during the Regional Exchange or in other forums. To facilitate the exchange of documents and expertise, an online working space will be set up thereby reducing the onsite meetings of the group members to a minimum. This platform will have working functionalities (board, library, wiki, shared document, chat, blog, profile management, calendar) as well as content manager capabilities so as to share the knowledge generated with all interested parties.

- 3.14 **Expected results of the project.** Inform policy makers and regulators in LAC in the design of national cyber law legislation and regulation taking into account the state of the art of the topic in the Region, as well as international lessons learned. Specific results include: (i) establishment of regional Working Groups on the following topics: capacity building and awareness; regulation and legal framework, policies and governance model; protection of critical infrastructure, and citizen security in the cyberspace; (ii) a diagnosis of the most important challenges and provision of recommendations to be included as part of the cyber security agenda and strategies in the Region; and (iii) creation of Regional Exchange on cyber security.

Table 3.1: Indicative results matrix

Output	Indicator	Base Line	Target at the end of the TC	Means of verification
Knowledge documents have been produced	Number of Documents	0	3 (regional diagnosis, international best practices document, regional maturity gap (gap analysis))	IDBDOCS
A multi-stakeholder regional exchange on cyber security established	Number of regional meetings organized	0	2	Regional meeting reports
Thematic working groups created	Number of working groups created	0	4	Working groups consultants reports
Outcome				
Policy makers and regulators have a better understanding of the most important challenges related to cyber security and are implementing initiatives in the field	Number of countries that set up new cyber security strategies	0	4	TC Final evaluation document

Table 3.2: Indicative budget (in US\$)

Budget line	Total	Year 1	Year 2	Year 3	Broadband Special Program	Citizen S Special Program
Component 1. Knowledge generation and dissemination	375,000	375,000	0	0	187,500	187,500
Activity 1. International Best Practices	44,000	44,000				
Activity 2. Diagnosis cyber security	188,000	188,000				
Activity 3. Gap analysis	64,000	64,000				
Activity 4. Experts roundtable	28,000	28,000				
Activity 5: Dissemination	51,000	51,000				
Component 2. Regional Exchange	199,800	99,900	99,900	0	99,900	99,900
Activity 1. 1st. Regional Exchange	99,900	99,900	0			
Activity 2. 2nd Regional Exchange	99,900		99,900			
Component 3. Thematic Working Groups (4)	330,200	77,400	173,400	79,400	165,100	165,100
Working Groups post 1st. Regional Exchange (2)	154,000	60,000	94,000			
Working Groups post 2nd Regional Exchange (2)	154,000		77,000	77,000		
Online platform	22,200	17,400	2,400	2,400		
Monitoring and evaluation	55,000		25,000	30,000	27,500	27,500
Contingencies	40,000	10,000	20,000	10,000	20,000	20,000
Total US\$	1,000,000	562,300	318,300	119,400	500,000	500,000

- 3.15 A midterm evaluation will be conducted to ascertain whether the project is advancing in accomplishing its objectives. This evaluation will be carried out based on personal interviews to the cyber security authorities who participated in the first Regional Exchange. This in-depth questionnaire will inquire, among other things, on the relevance

of the topics treated, the usefulness of the knowledge documents produced as well as the quantity and quality of expertise exchanged. After the last activity, a final evaluation will be completed including both personal interviews and a focus group comprised of at least one cyber security authority per Bank region to assess the overall impact of the project.

IV. EXECUTING AGENCY AND EXECUTION STRUCTURE

- 4.1 Due to the innovative nature and regional focus of this Technical Cooperation, it will be executed by the Bank through IFD/ICS. Since this TC will be the first initiative of the Bank in the field of cyber security, it is particularly important that the knowledge generated is closely monitored by the Bank's specialists and benefits them as well as the Region's cyber security authorities. This will facilitate not only the design of future initiatives but also the identification of potential partners. When contracting consulting services, Bank procurement policies as defined in GN-2350-9 will be followed.

V. PROJECT RISKS AND ISSUES

- 5.1 The supreme authority in cyber security is not clearly defined in some of the countries of the Region, while in others several government institutions share the responsibility thus making it difficult to identify the right counterpart for the initiative. This risk will be mitigated by conducting direct consultations with the respective governments through the Bank's country offices. The Bank will place special care in defining the participants in all project activities to ensure the appropriate country representation. In addition, a list of the participants in the latest cyber security events organized by ITU, OAS and WEF will be used as a starting point.
- 5.2 Activity 2 in Component 1 is based on voluntary participation of eight countries in a cyber-security diagnosis. Although the advice received by participating countries in exchange for their time commitment will be a strong incentive to participate, there is the risk of insufficient demand to complete the eight spots. If the call for volunteer countries does not generate a positive response from at least 4 of them, a subsidiary criterion to select these eight countries will be used based on proactively engaging all countries which might include offering the opportunity of hosting one of the Thematic Working Groups' onsite activities.
- 5.3 The Maturity Gap will identify weaknesses in the national cyber security policies that may generate negative reactions and lack of motivation to participate in a Regional Exchange. This risk will be mitigated by engaging the countries in the activities from their inception and throughout the process so the findings result from a team effort that includes the countries' contributions and the final results are anticipated.
- 5.4 The set up and consolidation of the Thematic Working Groups may face the challenge of attracting enough interested countries to make the exchanges valuable for all participants. This risk will be mitigated by selecting recognized experts to lead each of the Working Groups and by actively involving the countries in the agenda of each group.
- 5.5 The sustainability of this cyber security regional effort is not guaranteed after this technical cooperation is completed. This risk will be mitigated by making the regional exchanges a valuable coordinating space for regional cyber security efforts. Given the relevance of the field for their socio-economic progress, LAC countries will be motivated to assure that at least certain activities will be undertaken to maintain this effort functioning.

VI. EXCEPTIONS TO BANK POLICY

- 6.1 No exceptions to Bank policy are foreseen.

VII. ENVIRONMENTAL AND SOCIAL CLASSIFICATION

- 7.1 It is not foreseen that there will be environmental or social risks associated to the implementation of this project. Classification of this project is expected to be "C". No environmental assessment studies or consultations are required for Category "C" operations (please see link: [IDBDocs#37852344](#)).

REQUIRED ANNEXES:

- **Annex I - Terms of Reference:** [IDBDocs#38157278](#)
- **Annex II - Acquisitions Plan:** [IDBDocs#38157323](#)

TERMS OF REFERENCE
(Consulting Firm)

IFD/ICS

RG-T2380: Cyber Security: Setting the Ground for a Secure Cyber-Environment in Latin America and the Caribbean

Component 1: knowledge generation and dissemination

I. BACKGROUND

- 1.1 **Justification.** In recent years, the Information & Communication Technologies arena witnessed the emergence of a new but important concept entitled cyberspace. The cyberspace represents the way in which people, companies, government and machines communicate with each other and carry out transactions among themselves. While the advantages of living in a cyber-environment are overwhelmingly positive - in that it rewards innovation and empowers entrepreneurs, builds better governments and expands accountability - as in other sectors, cyberspace is also associated with numerous negative externalities which can enable specific harms such as information robbery, cyber terrorist attacks or cyber-espionage which can severely endanger citizen security and disrupt a country's economic wellbeing.
- 1.2 In January 2012, the World Economic Forum launched the initiative "Partnering for Cyber Resilience" which, among other principles, states that "countries need to set up initiatives for a comprehensive management of cyber-risks". 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. 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), the IDB will provide technical support through these consulting services to begin exploring ways by which Latin America and the Caribbean approach and address this very critical and timely issue.
- 1.3 The objective of this technical cooperation is to assist beneficiary countries¹ in the design of national Cyber Security strategies according to the most recognized international standards thereby strengthening citizen security. An improved legal and regulatory framework (harmonized regionally and compliant with international standards) as well as more updated and shared cyber security information are also expected to foster interaction and transaction among the different stakeholders (government, civil society, business community and academia), thus promoting more efficient public and private service delivery to individuals and businesses.

¹ This TC will focus on all Latin American and Caribbean countries that are members of the IDB.

- 1.4 The activities comprised in the project in reference are divided into three main components: (i) knowledge generation and dissemination; (ii) regional exchange; and (iii) working groups for institutional capacity building. Additionally, there will be specific activities for training and dissemination. These terms of reference define the required background and expertise, as well as the objectives, activities and the products to be carried out and delivered by a Consulting Firm hired under the project. This product corresponds with to Component I of the Regional project in reference.

II. CONSULTANCY OBJECTIVES

- 2.1 The objective of this consultancy is to undertake the tasks associated to the first component of this project, specifically, to find out the status of cyber security in Latin America and the Caribbean by identifying the progress made by each country towards a sound cyber security strategy, who are the main actors and what the needs in each of the countries are. As part of this component an analysis of the most recognized international experiences in cyber security will be conducted to be used as a reference by Latin American and Caribbean countries so that specific lessons learned can be identified.
- 2.2 The IDB is determined to assist beneficiary countries in the design and implementation of national Cyber Security strategies according to the most recognized international standards. An improved legal and regulatory framework following international standards as harmonized as possible regionally is also expected to foster interaction and transaction among the different stakeholders, thus promoting more efficient public and private service delivery to individuals and businesses.
- 2.3 IDB actions in the field are guided by the document *“From cyber security to cyber-crime: A framework for analysis and implementation”*² by Antonio García-Zaballos and Félix González where five pillars are defined in order to design a holistic cyber security plan (Point 3.5 of this document enumerates the five pillars). In addition, three Strategic objectives underline this support from the IDB to the LAC region in the area of Cyber Security (prevention, detection and reaction): (i) prevent cyber-attacks from taking place; (ii) reduce national vulnerabilities to cyber-attacks; and (iii) minimize damage and recovery time from cyber-attacks occurred. Additionally, through this consultancy, the Bank wants to help the selected countries to define strategies that protect the critical infrastructure and critical information.
- 2.4 Advanced international experiences in cyber security will let LAC countries to draw valuable lessons from both successes and failures from other regions. By analyzing the cyber security situation and the lessons learned from leading countries such as USA, Israel, South Korea and the EU, and comparing it with that of Latin America and the Caribbean, important knowledge will be generated and put a the service of cyber security leaders on the LAC region in order to support the design of sound cyber security policies and legal and regulatory frameworks.

² See Technical Note [IDBDocs#38133436](#).

III. ACTIVITIES AND PRODUCTS

- 3.1 The three activities of component 1 included in this consulting contract are the following:
- 3.2 **Activity 1: international best practices.** This activity will document the experiences of the 4 advanced countries in cyber security worldwide (USA, Israel, South Korea and one selected country from the EU country Members) in terms of capacity building and awareness, regulation and legal framework, policies, governance model (CERTs) and protection of critical infrastructure (also by means of deployment of cyber infrastructure). This analysis will provide a detailed description on lessons learned subject to being applied in the LAC Region. Detailed information will be analyzed for each country on each of the five pillars mentioned with particular emphasis on the results accomplished and the lessons learned for Latin American and Caribbean countries. A special chapter on the financial efforts made by these countries in order to set up sound cyber security policies should be included along with information to build a business case that justifies the government investments in cyber security plans.
- 3.3 **Activity 2: diagnosis of cyber security in Latin America and the Caribbean.** Through a structured survey, a cyber-security profile of the four sub-regions where the Bank is working will be elaborated including main actors, most critical threats, legal and regulatory framework, policies and initiatives in place as well as human resources capacity. The study will identify the main weaknesses of the Region's cyber security plans and include recommendations to design cyber security policies, laws and regulations that tackle the main risks and threats identified. To do so, a total of eight countries will be selected: two from the Caribbean Region, two from the Central American Region, two from the Andean Region and two from the Southern cone. To select the countries, a call for volunteer countries willing to do the necessary effort will be launched. Given the valuable free expert advice that participating countries will receive, more than the planned 2 countries per region are expected to volunteer. The two spots per region will be allocated on a first-come-first-serve basis to those that express their commitment first. The survey will be undertaken by conducting on-site structured interviews with cybersecurity authorities, civil society organizations, academics and businessmen. The study will be structured based on the five-action pillars defined as key elements for a holistic cyber security plan by the IDB in the document, "From cyber security to cyber-crime: A framework for analysis and implementation"³ by Antonio García-Zaballos and Félix González. These pillars are: (i) capacity building and awareness; (ii) regulation and legal framework; (iii) policies; (iv) governance model/CERT (Computer Emergency Response Team); and (v) infrastructure (software and hardware). Special emphasis will be placed in identifying the main attacks suffered by each country and the economic impact of those attacks.

³ See Technical Note [IDBDocs#38133436](#).

- 3.4 **Activity 3: gap analysis between the LAC Region and the leading countries.** Based on the diagnosis conducted in Activity 2, the document will include a gap analysis that will showcase where the Latin American and Caribbean countries stand when compared with the most advanced countries in the world. This gap analysis will be a valuable tool to guide the design of cyber security efforts in the region. Among other contributions, the study will identify the minimum standards that any national cyber security strategy should meet in order to protect its citizens from the most common cyber-threats and include a special chapter on the legal and regulatory framework for cyber security. As an annex to this chapter a model law will be proposed to be used as a template for all LAC countries. As in the case of the cybersecurity diagnosis the survey to conduct the gap analysis will be structured based on the five-action pillars indicated in Activity 2. The survey will cover all Latin American and Caribbean countries and will be done through a comprehensive online questionnaire that will capture the opinion of all relevant stakeholders: government authorities responsible for cyber security, heads of business chambers and associations, most recognized academics and researchers, the leaders of civil society organizations with an active role in citizen security or cyber security. In addition, a template for the design of a cyber security strategy based on the best practices analyzed will be included in the document generated as part of this activity.
- 3.5 The documents produced under activities 1, 2 and 3, will be edited and published digitally to facilitate its dissemination not just among the different participants of the activities planned but also among the cyber security community of Latin American and the Caribbean. These documents will be made available at the online spaces of the Broadband and Citizen Security Initiatives and will be promoted at events organized by both initiatives. In addition, an online platform to facilitate knowledge exchange and collaboration will be launched thereby facilitating the dissemination of all knowledge products generated by this technical cooperation.
- 3.6 **Expected results.** As a result of this consultancy, the following outputs are expected (with the level of detail explained in the activities description): (i) an International Best Practices in cyber security document; (ii) a diagnosis of the status of cyber security in Latin America and the Caribbean; (iii) a cyber security gap analysis between the LAC Region and the most advanced countries, including a cyber security model law for the LAC region.

IV. CHARACTERISTICS OF THIS CONSULTANCY

- 4.1 **Type of Consultancy:** Consulting Firm
- 4.2 **Starting date and duration:** Upon contract signing, 6 months
- 4.3 **Working place/travels:** This consultancy will be carried out by a consulting firm. Although the tasks may be carried out in the country of origin, the firm will be required to travel to all the selected countries to conduct the field work, meet with the relevant authorities and to present and disseminate the results.

- 4.4 **Qualifications:** The firm will have extensive experience in the information and communication technologies field, with senior team members involved in projects in LAC and other developing regions. Specific experience in all aspects of cyber security both at policy advice level and at operational level, advising the design and implementation of cyber security strategies at the public or private sectors. The firm should also have background on projects involving countries from different regions of the world where the transfer of knowledge and lessons learned was important. The firm must have a proven capability to deliver detailed and accurate recommendations, particularly in strategic and regulatory aspects of cyber security, and of understanding sector trends, since the results of this component will serve as critical inputs for the development of other components in the framework of this project.

V. METHOD OF PAYMENT

- 5.1 Payment will be made as per the following schedule, upon approval by the Team Leader responsible for this project (see item VI below):
- 5.2 **Schedule of payments:**
- a. 25% upon contract signature;
 - b. 20% upon approval of draft report (i);
 - c. 25% upon approval of draft report (ii)
 - d. 30% upon approval of draft report (iii)

VI. COORDINATION

- 6.1 The supervision and coordination of this consultancy will be the responsibility of Mr. Miguel Porrúa, Modernization of the State Lead Specialist, (IFD/ICS), Team Leader of this operation, mporrúa@iadb.org tel. (202) 312-4102.

TERMS OF REFERENCE

(Thematic Working Group Consultant – There will be 4 countries like this one. One per thematic area)

IFD/ICS

RG-T2380: Cyber Security: Setting the Ground for a Secure Cyber-Environment in Latin America and the Caribbean

Component 3. Thematic Working Groups

I. BACKGROUND

- 1.1 **Justification.** In recent years, the Information & Communication Technologies arena witnessed the emergence of a new but important concept entitled cyberspace. The cyberspace represents the way in which people, companies, government and machines communicate with each other and carry out transactions among themselves. While the advantages of living in a cyber-environment are overwhelmingly positive - in that it rewards innovation and empowers entrepreneurs, builds better governments and expands accountability - as in other sectors, cyberspace is also associated with numerous negative externalities which can enable specific harms such as information robbery, cyber terrorist attacks or cyber-espionage which can severely endanger citizen security and disrupt a country's economic wellbeing.
- 1.2 In January 2012, the World Economic Forum launched the initiative “Partnering for Cyber Resilience” which, among other principles, states that “countries need to set up initiatives for a comprehensive management of cyber-risks”. 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. 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), the IDB will provide technical support through these consulting services to begin exploring ways by which Latin America and the Caribbean approach and address this very critical and timely issue.
- 1.3 The objective of this technical cooperation is to assist beneficiary countries⁴ in the design of national Cyber Security strategies according to the most recognized international standards thereby strengthening citizen security. An improved legal and regulatory framework (harmonized regionally and compliant with international standards) as well as more updated and shared cyber security information are also expected to foster interaction and transaction among the different stakeholders (government, civil society, business community and

⁴ This TC will focus on all Latin American and Caribbean countries that are members of the IDB.

academia), thus promoting more efficient public and private service delivery to individuals and businesses.

- 1.4 The activities comprised in the project in reference are divided into three main components: (i) knowledge generation and dissemination; (ii) regional exchange; and (iii) working groups for institutional capacity building. Additionally, there will be specific activities for training and dissemination. These terms of reference define the required background and expertise, as well as the objectives, activities and the products to be carried out and delivered by a Project Manager hired under the project.
- 1.5 As part of the component 3 mentioned in the previous paragraph, two Thematic Working Groups (TWG) will be created after each regional exchange. Countries interested in joining these groups will be able to maintain in-depth discussions throughout the year aiming at exchange knowledge and strengthening the capacity of their human resources in the matter. These discussions will be guided by an expert consultant and will count on the contributions of knowledgeable professionals in the respective field.

II. CONSULTANCY OBJECTIVES

- 2.1 The objective of this consultancy is to provide technical guidance and manage the activities of the Thematic Working Group “TOPIC TO BE DEFINED BY COUNTRIES IN REGIONAL EXCHANGE I” within the Regional Technical Cooperation “Cyber Security: Setting the Ground for a Secure Cyber-Environment in Latin America and the Caribbean” (RG-T2380)

III. MAIN ACTIVITIES AND PRODUCTS

- 3.1 In order to accomplish the consultancy objective, the consultant will carry out the following specific activities:
 - The Consultant will produce an executive paper on the matter in order to present the topic to the TWG members and trigger the discussions with the group participants.
 - The Consultant will set up and manage an online working space in a platform provided by the Bank. As part of this responsibility, the consultant will produce an online library of relevant documents on the topic which will be used as bibliography to support the group discussions.
 - The Consultant will elaborate a one-year plan of activities that will include: joint research to identify the most advanced experiences in the region, knowledge exchange activities, online expert presentations, onsite workshop on the topic.
 - In coordination with the project manager, the consultant will define the agenda for the onsite workshop in the topic, identifying the leading countries

and experts to present in the workshop and overseeing the preparation of all presentations and documents to be distributed during the activity.

- The Consultant will also produce a TWG document on the topic that will report on the status of the topic in the region, the activities undertaken by the TWG, the impact of those activities on each country and operations plan of the group for the next year.
- The Consultant will provide general advice on the topic to IFD/ICS in undertaking Technical Cooperation RG-T2380, occasionally participating in meetings and making limited contributions to the production of documents.

IV. CHARACTERISTICS OF THIS CONSULTANCY

- **Consultancy Category & Modality:** International Individual Consultancy-PEC
- **Contract Duration:** 12 months starting September 1, 2014 to September 1, 2015.
- **Place(s) of work:** Consultant's own facilities. Due to the responsibilities that this consultancy entails, the consultant can be asked to travel to the Bank's headquarters or any member countries.

Qualifications

- **Academic Degree/level:**
 - Bachelor's Degree in Systems Engineering, Telecommunications or other Information Technology related topics.
 - Masters degree in cyber security, ICTs public policies or any of the above-mentioned areas desired.
- **Years of professional experience:** The consultant should have at least 5 years of professional experience cyber security related positions at either the private or public sector. Public Sector experience desired and cyber-security policy related experience a plus.
- **Language:** Excellent analytical and writing communication skills in English and Spanish. French is desirable.
- **Areas of expertise:** Citizen Security, Cyber-Security, e-Government, Telecommunications, Information Technologies, International Development.

V.METHOD OF PAYMENT

5.1 Schedule of payments:

- 20% Upon contract signing
- 20% upon submission and approval of activities report 1
- 20% upon submission and approval of activities report 2
- 20% upon submission and approval of activities report 3
- 20% upon submission and approval of final report.

VI.COORDINATION

- 6.1 The Consultant will report to Mr. Miguel Porrúa, Modernization of the State Lead Specialist, (IFD/ICS), Team Leader of this operation, mporrúa@iadb.org tel. (202) 312-4102.

PROCUREMENT PLAN

No. Ref.	Description and type of the procurement contract	Estimate d contract Cost US\$	Procure ment method ¹	Review (ex- ante or ex- post)	Source of financing and percentage		Prequali- ficación (Yes/No)	Estimated dates		Status (pending, in progress, awarded, cancelled)	Comments
					IDB %	Local / other %		Publication of specific procurement notice	Completion of contract		
1	GOODS										
	N/A										
2	WORKS										
	N/A										
3	NON-CONSULTING SERVICES										
	Component 1. Activity 4 Experts round table	28,000	PC	ex-post	100%	0%	No	N/A	2014	Pending	
	Component 2. Activity 1 Regional Exchange 1 Plane tickets and perdiem	99,900	PC	ex-post	100%	0%	No	N/A	2014	Pending	
	Component 2. Activity 2 Regional Exchange 2 Plane tickets and perdiem	99,900	PC	ex-post	100%	0%	No	N/A	2015	Pending	
	Component 3 Workshops year 2 (2)	104,000	PC	ex-post	100%	0%	No	N/A	2015	Pending	
	Component 3 Workshops year 3 (2)	104,000	PC	ex-post	100%	0%	No	N/A	2015	Pending	
4	CONSULTING SERVICES (Individual)										
	Component 1: Dissemination	51,000	IICC	ex-post	100%	0%	No	N/A	2014	Pending	
	Component 3: Thematic Working Group Consultant 1.	30,000	IICC	ex-post	100%	0%	No	N/A	2015	Pending	
	Component 3: Thematic Working Group Consultant 2.	30,000	IICC	ex-post	100%	0%	No	N/A	2015	Pending	
	Component 3: Thematic Working Group Consultant 3.	30,000	IICC	ex-post	100%	0%	No	N/A	2016	Pending	
	Component 3: Thematic Working Group Consultant 4.	30,000	IICC	ex-post	100%	0%	No	N/A	2016	Pending	
	Component 3: Online	22,200	IICC	ex-post	100%	0%	No	N/A	2016	Pending	

No. Ref.	Description and type of the procurement contract	Estimated contract Cost US\$	Procurement method ¹	Review (ex-ante or ex-post)	Source of financing and percentage		Prequalification (Yes/No)	Estimated dates		Status (pending, in progress, awarded, cancelled)	Comments
					IDB %	Local / other %		Publication of specific procurement notice	Completion of contract		
	platform and hosting										
	Monitoring and evaluation	35,000	IICC	ex-post	100%	0%	No	N/A	2016	Pending	
5	CONSULTING SERVICES (Firms)										
5.1	Component 1: Knowledge generation and dissemination. Activities 1, 2 and 3.	296,000	QCBS	ex-post	100%	0%	No	N/A	2014	Pending	

¹ **Goods and Works:** **ICB:** International competitive bidding; **LIB:** limited international bidding; **NCB:** national competitive bidding; **PC:** price comparison; **DC:** direct contracting; **FA:** force account; **PSA:** Procurement through Specialized Agencies; **PA:** Procurement Agents; **IA:** Inspection Agents; **PLFI:** Procurement in Loans to Financial Intermediaries; **BOO/BOT/BOOT:** Build, Own, Operate/Build, Operate, Transfer/Build, Own, Operate, Transfer; **PBP:** Performance-Based Procurement; **PLGB:** Procurement under Loans Guaranteed by the Bank; **PCP:** Community participation procurement. **Consulting Firms:** **QCBS:** Quality- and Cost-Based Selection **QBS:** Quality-Based Selection **FBS:** Selection under a Fixed Budget; **LCS:** Least-Cost Selection; **CQS:** Selection based on the Consultants' Qualifications; **SSS:** Single-Source Selection. **Individual Consultants:** **NICQ:** National Individual Consultant selection based on Qualifications; **IICC:** International Individual Consultant selection based on Qualifications.