TECHNICAL COOPERATION DOCUMENT (TC-DOCUMENT)

REGIONAL

I. BASIC INFORMATION

Country:	Regional
TC Name:	Cyber Security: Setting the ground for a secure cyber-environment
TC Number:	RG-T2380
Team Leader/Members:	Antonio García Zaballos (Team Leader, IFD/CTI); Nathalie Alvarado (Co-Team Leader IFD/ICS); Felix Gonzalez (IFD/CTI); Miguel Porrua (IFD/ICS); Ricardo Lesperance (IFD/ICS); Nathalia Foditsch (IFD/CTI); Jiyoun Son (IFD/CTI); and Cecilia Bernedo (IFD/CTI).
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:	The Bank through the division of Competitiveness and Innovation Division (IFD/CTI) (in coordination with Institutional Capacity of the State Division (IFD/ICS))
Donors providing funding:	
Financing plan:	**IDB (programa especial de banda ancha):** US$1.000,000
Local counterpart:	**Local:** US$ 0 **Total:** US$1.000,000
Execution period:	36 months **Disbursement period:** 39 months
Required start date:	August, 2013
Types of consultants:	Individual Consultants, Consulting firm
Prepared by Unit:	IFD/CTI & IFD/ICS
Unit of Disbursement Responsibility:	IFD/CTI
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. To this end, the IDB will work towards strengthening institutions, and has specifically recognized 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). 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 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.

2.2 This panorama of devices and human beings connected is shaping a new ecosystem of players and elements that make the connectivity possible. The elements of the *ecosystem* and the use of the Internet are determining a new concept in the ICT arena that is the *cyberspace.* The *cyberspace* truly represents the way in which people, companies, government and machines communicate with each other and carry out transactions among them. 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. As in other sectors, those externalities can turn out to be negative and specific harms such as information robbery, *cyber terrorist* attacks or *cyber espionage* can occur.

2.3 The World Economic Forum launched the initiative "Partnering for Cyber Resilience" in January 2012. Among other principles to protect the world from cyber-attacks, the document 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[2].

2.4 **Objectives.** The ultimate objective of the project is 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 (harmonized regionally and compliant with international standards) 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.

---

[1] Pathways to Innovation: Policy approaches for accelerating broadband deployment and adoption in Latin America and the Caribbean.

[2] http://www.itu.int/cybersecurity/.

2.5 To achieve that goal, there must be three strategic objectives that match the cyber security cycle (prevention, detection and reaction): (i) prevent cyber-attacks; (ii) reduce national vulnerabilities to cyber-attacks; and (iii) minimize damage and recovery time from cyber-attacks occurred. In addition, we will be helping the selected countries to define strategies that protect the critical infrastructure and the critical information.

2.6 A key aspect of a sound Cyber Security strategy will be the modernization of the legal and regulatory framework. To support the efforts in this area, a regional harmonized legal and regulatory framework for CyberSecurity will be defined by analyzing the lessons learned from leading countries such as USA, Israel, South Korea and the EU Members. The harmonized aspect is crucial to guarantee homogeneity across countries in the region to facilitate cyber-crime prosecution.

2.7 The contribution of the Bank to accompanying countries in their *cyber security* efforts must be doubled. First, the Bank should help countries conduct an assessment of the current status of *cyber security* and facilitate a regional dialogue based on the findings of this assessment. Secondly, and based on that regional dialogue, the Bank should contribute 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 main components: (i) knowledge generation and dissemination; (ii) regional dialogue; and (iii) working groups for institutional capacity building.

3.2 **Component 1: knowledge generation and dissemination.** The objective of this component is 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 are the needs in each of the countries. 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.

3.3 **Activity 1: international Best Practices**. This activity will document the experiences of the 4 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 (CERTs) and protection of critical infrastructure (also by means of deployment of cyber infrastructure). This analysis will provide a detailed description on lessons learned susceptible of being applied in 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 resources capacity. The document will include recommendations to design *cyber security* policies, laws and regulations that tackle the main risks and threats identified. To do so, a total of 8 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.

3.5 **Activity 3: gap analysis between the LAC Region and the leading countries.** 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. In addition, the study will identify the minimum standards that any national *cyber security* strategy should meet in order to protect its citizens from the most comment cyber-threats. This gap analysis will be a valuable tool to guide the design of *cyber security* efforts in the region.

3.6 **Activity 4: experts roundtable.** The report described previously will be analyzed by a group of recognized experts representing the main *cyber security* stakeholders (government, companies, academia, NGOs) along with the IDB experts in order to identify potential areas of action and the value-added that the IDB can bring to the table. 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 management and staff with the necessary business intelligence prior to the dialogue with the region's *cyber security* authorities.

3.7 **Component 2: Regional Dialogue 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. Taking advantage of the current agenda of Citizen Security and Public Management Clusters of IFD/ICS as well as that of the Broadband Initiative of IFD/CTI, a regional meeting of all relevant *cyber security* stakeholders will be organized with the objective of analyzing status of *cyber security* in Latin America and the Caribbean, potential initiatives to improve, and mechanisms to coordinate and cooperate.

3.8 **Activity 1: First Regional Dialogue on Cyber Security Policies.** This first Regional Dialogue will be attended by *cyber security* authorities, ICT companies, academics, representatives from the organized civil society, international experts and relevant international organizations. During this first workshop, the Regional Diagnosis Report, the International Experiences Document and the Maturity Gap Analysis will be used as the triggers of a multi-stakeholder dialogue aiming at defining the main components of a reliable national *cyber security* strategy.

3.9 Discussions held during this Regional Dialogue will allow the identification of those areas of *cyber security* where the Latin American and Caribbean countries require specific support.

3.10 This Regional Dialogue will also offer those International Organizations that are active in the field of *cyber security* such as the OAS, WEF, ITU, UNCTAD and others to present their respective initiatives and to coordinate efforts among themselves and with the IDB.

3.11 **Activity 2: Second Regional Dialogue on Cyber Security Policies**. This Second Regional Dialogue 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 Dialogue, it will be a multi-stakeholder meeting with the participation of international experts and organizations.

3.12 **Component 3: thematic working groups.** After each Regional Dialogue on *cyber security* Policies five key topics will be defined as critical to advance the *cyber security* agenda (capacity building and awareness, regulation and legal framework, policies, governance model and protection of critical infrastructure also including deployment of infrastructure). A working group on each of the five topics will be set up with the leadership of a recognized expert. Each group will be comprised of representatives of all interested countries and will be endowed with resources to conduct specific research and training in the area of focus.

3.13 Each Thematic Working Group will undertake onsite and online workshops and develop specific research concentrated in the target topic. These Working 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 whole region and to present during the Regional Dialogue.

3.14 **Expected results of the project.** The *regional framework for cyber laws* produced as a result of this project will 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 LAC Region. Particularly the technical cooperation will provide recommendations on standards that should be included as part of the cyber security policies and strategies according to the lessons learned from the leading countries. Specific results include:

a. Establishment of regional Working Groups on the following topics: capacity building and awareness, regulation and legal framework, policies, governance model and protection of critical infrastructure.
b. A diagnosis on the most important challenges in the Region and provision of recommendations to be included as part of the *cyber security* agenda and strategies.
c. Creation of Regional Dialogue on *cyber security*.

Table 3.1: Indicative results matrix

Suggested Indicator (outcome)	Base Line	Target at the end of the TC
Knowledge generation and dissemination	0	1 regional diagnosis 1 international best practices document and regional maturity gap
A multi-stakeholder regional dialogue on *cyber security* established	0	8 LAC countries have a better understanding of the most important challenges related to *cyber security* and are implementing initiatives in the field.
Institutional strengthening in *cyber security*	0	5 Thematic Working Groups in operation. Each will be comprised of a minimum of 8 countries with 2 representatives per country,

Table 3.2: Indicative budget (in US$)

Budge line	Year 1	Year 2	Year 3	Total
Knowledge generation and dissemination	**251,000**	**251,000**		**502,000**
International consultants (2)	200,000	200,000		400,000
Travel consultants	20,000	20,000		40,000
Experts roundtable	25,000	25,000		50,000
Graphic design and editing	6,000	6,000		12,000
Regional Dialogue	**66,700**	**66,700**		**133,400**
Flight tickets	39,000	39,000		78,000
Perdiem	11,700	11,700		23,400
Translation and interpretation	10,000	10,000		20,000
Document printing	6,000	6,000		12,000
Thematic Working Groups (4)			**269,600**	**269,600**
International consultants (4)	--		100,000	100,000
Workshops (6)	--		120,000	120,000
Online platform	--		49,600	49,600
Contingencies	**45,000**	**25,000**	**25,000**	**95,000**
Total	**362,700**	**342,700**	**294,600**	**1,000,000**

IV. EXECUTING AGENCY AND EXECUTION STRUCTURE

4.1 This Technical Cooperation will be executed by the Bank through the Division of Competitiveness and Innovation Division (IFD/CTI) (in coordination with the Division of Institutional Capacity of the State (IFD/ICS)).

V. PROJECT RISKS AND ISSUES

5.1 The ultimate 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. The project must place special care in defining the list of participants in all the activities to ensure the appropriate country representation.

5.2 The Maturity Gap will identify weaknesses at the national *cyber security* policies that may generate negative reactions and lack of motivation to participate in a

Regional Dialogue. The countries should be engaged in the activities from inception in order to avoid potential conflicts.

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).