Technical Cooperation Document (TC-DOCUMENT)

REGIONAL

I. Basic Information

Country:	Regional	
TC Name:	Development of Critical Infrastructure Protection (CIP) Plan	
TC Number:	RG-T2458	
Team Leader/Members:	Antonio Garcia Zaballos (Team Leader, IFD/ICS); Nathalia Foditsch (IFD/ICS); Jiyoun Son (IFD/ICS); Felix Gonzalez (IFD/ICS), and Cecilia Bernedo (IFD/ICS)	
TC Taxonomy:	Research and Development (RD)	
Authorization TC date:	April, 2014	
Donors providing funding:	Knowledge Partnership Korea Fund for Technology and Innovation (KPK)	
Beneficiary:	Latin American and Caribbean Region (LAC)	
Executing agency and contact name:	Inter-American Development Bank, Antonio García (antoniogar@iadb.org)	
IDB Funding Requested:	BID:	US$540,000
Local counterpart funding:	Local: Republic of Korea (in kind)	US$130,000
	Total:	**US$670,000**
Execution period:	20 months **Disbursement period:** 24 months	
Required start date:	June, 2014	
Types of consultants:	Firm and individual consultants	
Prepared by Unit:	Division of Institutional Capacity of the State (IFD/ICS)	
Unit of disbursement responsibility:	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. 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 Communications Technology (ICT) sector (par.5.21 of the referred to Sector Strategy). Consistent with the Strategy, the Bank has been working in the design and implementation of a Broadband Platform to accelerate the penetration rate and usage of broadband services in the Region.	

II. OBJECTIVES AND JUSTIFICATION OF THE TC

2.1 The LAC Region is growing at a rapid pace in the use of the Internet and the deployment of broadband, and has enormous potential to grow further. According to the Internet World Statistics (IWS), the number of the Internet users in the LAC Region amounts to 254.91 million or 10.4% in the world. From 2000 to 2012, the LAC Region took third place (1,311%) in the rate of an increase in the number of the Internet users, following Africa (3,607%) and the Middle East (2,640%). SNL Kagan, a market research institution, predicts the number of households that subscribe to broadband in the LAC region will record an average annual growth rate of 11.9% by 2015, surpassing that of the Middle East (11.7%) and the Asia-Pacific (10.4%).

2.2 An increase in the Internet use is fueling cyber-attacks and cyber-crimes targeting national critical infrastructure, the backbone of a nation's security, economy, health and safety. Critical infrastructure are the assets, systems, and networks such as medical record information systems, energy grids, airport traffic control, transportation systems, gas pipeline networks, etc., which are, whether physical or virtual, so vital to the LAC Region. The incapacitation or destruction of this infrastructure would have a debilitating effect on national security, economic activities, public health or safety, or any combination thereof. The Organization of American States (OAS) reports that the rate of cyber-attacks levied in the LAC Region soared by 40% from 2011 to 2012 (Latin American and Caribbean Cybersecurity Trends and Government Responses, May 3, 2013).

2.3 The risk environment affecting critical infrastructure is complex and uncertain; threats, vulnerabilities, and consequences have all evolved over the last ten years. For example, critical infrastructure that has long been subject to risks associated with physical threats and natural disasters is now increasingly exposed to cyber risks. Growing interdependencies across critical infrastructure systems, particularly reliant upon information and communication technologies and their integration have increased the potential vulnerabilities to physical and cyber threats and potential consequences resulting from the compromise of underlying systems or networks. In an increasingly interconnected world, where critical infrastructure crosses national borders and global supply chains, the potential impact increases with the growth of interdependencies and a diverse set of threats to exploit them.

2.4 Cyber-attacks on critical infrastructure have significantly increased recently, targeting the Industrial Control Systems (ICS) that control national critical infrastructure for finance, transportation, energy, medicine, etc. Also, “hacktivist” activities with political or social motives loom large, exacerbating the increasing trend of cyber-threats. According to the OAS and Trend Micro, the number of security vulnerabilities reported by 51 business operators in the field of ICS security amounted to 171 in 2012 alone. In South America, SCADA[1] and VxWorks[2] are frequently used in protecting the ICS. However, since most of these systems are connected to the Internet, they often become the target of external attacks.

2.5····· While most countries in the LAC Region have organized and are operating Computer Security Incident Response Teams (CSIRT), cyber-attacks do not show any sign of a decrease. In addition, there is a lack of technical manpower and specialized organizations that are capable of effectively responding to well-organized and sophisticated cyber-attacks. The scarcity leads to difficulty in detecting cyber-attacks.

2.6····· Most importantly, a system to build capacity for information security must be put in place. The Critical Infrastructure Protection (CIP) system aims at not only going beyond simple incident response and reducing cyber-attacks themselves but also ensuring a secure operation of national infrastructures by: (i) establishing relevant legislation at national level; (ii) nurturing professionals; and (iii) promoting public awareness.

2.7····· A country should prepare and consistently strengthen mid- and long-term plans to establish a comprehensive national CIP plan, which will enable the country to build capacity to prevent, detect, respond to, and recover from cyber-attacks.

2.8 ·····**Objectives of the project.** The objectives of the TC are to develop a CIP plan applicable to countries in the LAC Region by surveying and analyzing the best practice cases of other nations and regions and to make recommendations for the seamless, practical implementation of the plan.

III. DESCRIPTION OF ACTIVITIES

3.1 The activities in the project are divided into four components: (i) conduct research on best practice cases of leading nations in the formulation and implementation of a CIP plan; (ii) conduct survey and analysis of the current status of CIP in the countries in the LAC Region that are aggressively pursuing ICT development such as Brazil, Argentina, Costa Rica, etc. and build regional capacity; (iii) provide recommendations for laws and institutions for CIP; and (iv) provide recommendations for the satisfaction of technological requirements for CIP.

3.2 **Component 1 – Conduct research on best practice cases of leading countries in CIP.** The objective of the component is to analyze best practice cases currently being implemented in countries that are exemplary in the field, such as EU (e.g., European Program for Critical Infrastructure Protection), Korea (e.g., Guidelines on Critical

[1] SCADA (Supervisory Control and Data Acquisition) is a system to control remote monitoring or collect data from supervisory control. The system supervises and controls decentralized facilities regarding transmission of electricity, petrochemical plants, iron processing, factory automation, and etc.

[2] VxWorks is a Real-Time Operation System (RTOS) developed by Windriver Systems. The system is often used for a spaceship or an aircraft.

Information and Communications Infrastructure Protection), and Israel (e.g., a centralist national critical infrastructure protection system) in order to understand the detailed information including background, impact, variables, etc. and identify the most suitable practice for countries in the LAC Region.

3.3 In order to take advantage of the results of the survey and analysis, it would be necessary to have a clear understanding of the current status of the relevant national and regional policies on CIP, laws and regulations, practices and principles, and challenges. Surveyed best practice cases and the results of analysis will be documented and made available on the website that will be set up to facilitate information sharing, serving as guidelines for CIP. The provision of guidelines will help governments in the LAC Region effectively protect critical infrastructure by establishing or improving legal framework and national policies, raising awareness, etc. International cooperation will also be needed to facilitate sharing the latest updates and reaching a consensus on adopting a best practice at the regional level. It will be promoted through a workshop and a site visit to one of the leading countries. Government officials from around ten LAC countries will be invited to participate in these activities with financial support of their trip.

3.4 **Component 2 – Conduct survey and analysis of the current status of CIP of LAC countries that are aggressively seeking ICT development such as Brazil, Argentina, Costa Rica, etc. and build regional capacity.** The objective of the component is to diagnose and analyze the status of CIP in countries in the LAC Region, thereby producing inputs for the development of the next two components. The study will consist of categorizing countries according to the level of ICT development and the recognition of the significant implication of cyber security. The scope of the survey will cover laws, the structure of organization in charge of promoting cyber security as well as ICT, technological readiness, human capacity and so on. A workshop will be held in association with a regional dialogue in a LAC country to share the outcome of the analysis.

3.5 **Component 3 – Provide recommendations for laws and institutions for CIP.** The objective of this component is to develop and recommend the procedures and elements of CIP-related laws and a set of regional guidelines. Based on the results from Components 1 and 2, recommendations for laws, guidelines, and programs tailored for the LAC region will be provided. Also, appropriate steps towards the establishment and operation of information security system in the public sector will be identified. An inter-governmental organization model, drawing upon effective and responsive cooperation among relevant Ministries and Agencies, will also be suggested.

3.6 **Component 4 – Provide recommendations for the satisfaction of technological requirements for CIP.** The objective of this component is to recommend procedures and methods for the establishment of a national Computer Security Incidents Response Team (CSIRT). Several best practice cases will be provided including the background of the establishment of the Korea Internet Incident Center (KISC) within the Korea Internet & Security Agency (KISA) and the current operational status will be elaborated. The basic requirement for technical equipment for KISC will be discussed. Also the team will provide advice on legally collecting traffic information from privately owned and operated telecommunication networks.

3.7 **Component 5 – Dissemination.** The objective of this component is to present the major findings and roadmap to execute the recommendations that are identified during the project. Dissemination will consist on a publication and an event to present the results.

3.8 **Expected results:** This project will enable a diagnosis of the current status and level of critical infrastructure protection in countries in the LAC Region. In addition, it will provide a model CIP plan for adoption by LAC countries, based on the knowhow from the leading CIP countries. Comprehensive mid- and long-term plans will be laid out for application to LAC countries and building a national information security system. Recommendations for how to build a legal and organizational foundation for implementing the plan will also be prepared. Ultimately, workshops accompanied by training opportunities will be held to disseminate knowledge and promote progress in countries across the LAC Region with a view to encouraging them to establish a CIP plan and related systems.

Table 3.1: Indicative Results Matrix

Suggested Indicator(Outcome)	Base Line	Target at the end of the TC
Conduct research on best practice cases of leading countries in CIP	0	1 Report identifying best practices and main points of critical infrastructure protection plans and its implementation activities of several exemplary countries
Conduct survey and analysis of current CIP status in countries in the LAC	0	1 Comparative diagnosis of CIP status of at least 4 countries in LAC.
Provide recommendations for laws and institutions for CIP	0	1 Report with set of recommendations, laws and other institutional suggestions for CIP
Provide recommendation for satisfaction of technological requirements for CIP	0	1 Report with methods for developing technological preparedness including the procedure of setting up and advancement of CSIRT, etc.

Table 3.2: Indicative Budget (Unit: US$)

Component	Activities	Sub-components			Funding Sources		Total
		Consulting	Travel & Accommodation	Others	IDB	Korea	
Component 1: Research on the best practices	Activity 1: survey and analysis of at least 3 countries with best practices	100,000	50,000		120,000	30,000	150,000
	Activity 2: site-visit training in one of advanced countries		50,000	20,000		70,000	70,000
Component 2: Survey and analysis of CIP status of LAC countries	Activity 1: survey and analysis of laws, policies, and technical measures to protect critical infrastructure	100,000	30,000		130,000		130,000
	Activity 2: Regional Workshops and Local Off-site Training Sessions	40,000	10,000		50,000		50,000
Component 3: Recommendations for laws and institutions	Activity: provide the master plan for critical infrastructure protection consisting of change of laws, organizational structure, institutional capacity building	140,000			140,000		140,000
Component 4: Recommendation for technological requirements	Activity: suggest technological measures to support effective prevention, detection and counteraction	120,000			90,000	30,000	120,000
Component 5: Dissemination	Activity: disseminate the result of consultancies			10,000	10,000		10,000
Total		**500,000**	**140,000**	**30,000**	**540,000**	**130,000**	**670,000**

IV. EXECUTING AGENCY AND EXECUTING STRUCTURE

4.1 Considering that the project is at regional level and needs extensive collaboration with different government institutions involved, the executing agency will be the IFD/ICS Division, which has broad experience working with the indicated institutions. IFD/ICS will operate in coordination with the Republic of Korea, which will inject in-kind contribution into the project.

V. PROJECT RISKS AND ISSUES

5.1 **Difficulty in collecting data from countries via survey.** Gathering of survey data from countries may be challenging since each country may consider the result of surveys confidential and, thus, be reluctant to share this information. Additionally, if there is insufficient data to come to a meaningful conclusion, the trustworthiness of the results themselves might be compromised. Therefore, an elaborate, inclusive communication strategy is required to encourage countries' understandings and involvement in the project.

5.2 **Applicability of the output.** The LAC Region may vary widely in implementing the comprehensive CIP plan, depending on the situation of each country and it is unlikely that any single recommendation would work for most countries as a prototype. Therefore, to make recommendations more applicable to a large number of countries, the output should be categorized at least into sub regional level or in accordance with its ICT development level.

VI. EXCEPTIONS TO THE POLICY OF THE BANK

6.1 There are no exceptions to the policy of the Bank.

VII. ENVIRONMENTAL STRATEGY

7.1 The nature of the TC that includes a survey expects no environmental and social risks associated with it. The operation is classified as Category "C," according to the Bank's classification toolkit. (see link: IDBDocs#38713289)