

## TECHNICAL COOPERATION DOCUMENT (TC-DOCUMENT)

### REGIONAL

#### I. BASIC INFORMATION

<b>Country:</b>	Regional
<b>TC Name:</b>	Development of Critical Infrastructure Protection (CIP) Plan against cyber-attacks
<b>TC Number:</b>	RG-T2458
<b>Team Leader/Members:</b>	Antonio Garcia Zaballo, Team Leader (IFD/ICS); Felix Gonzalez Herranz, Alternate Team Leader (IFD/ICS); Betina Hennig (LEG/SGO); Miguel Porrua (IFD/ICS); Enrique Iglesias (IFD/ICS); and Cecilia Bernedo (IFD/ICS)
<b>TC Taxonomy:</b>	Research and Development (RD)
<b>Authorization TC date:</b>	April, 2014
<b>Beneficiary:</b>	Latin American and Caribbean Region (LAC)
<b>Executing agency and contact name:</b>	Inter-American Development Bank, Antonio García ( <a href="mailto:antoniogar@iadb.org">antoniogar@iadb.org</a> )
<b>Donors providing funding:</b>	Knowledge Partnership Korea Fund for Technology and Innovation (KPK)
<b>IDB funding requested:</b>	BID: US\$540,000
<b>Local counterpart funding:</b>	Local: 0
	Other Funding: Republic of Korea ( <a href="#">in kind</a> ) <u>US\$130,000</u>
	<b>Total: US\$670,000</b>
<b>Execution period:</b>	20 months
<b>Required start date:</b>	August, 2014
<b>Types of consultants:</b>	Firm and individual consultants
<b>Prepared by Unit:</b>	Division of Institutional Capacity of the State (IFD/ICS)
<b>Unit of disbursement responsibility</b>	IFD/ICS
<b>TC included in country strategy:</b>	N/A
<b>GCI-9 sector priority:</b>	<b>TC included in CPD:</b> N/A 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)<sup>1</sup>, 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 expands vulnerability to cyber-attacks and cyber-crimes targeting national critical infrastructures, the backbone of a nation's security, economy, health and safety. Critical infrastructures include 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 any country. 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 recently targeted 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

---

<sup>1</sup> <http://www.internetworldstats.com/>

in the field of ICS security amounted to 171 in 2012 alone. In South America, SCADA<sup>2</sup> and VxWorks<sup>3</sup> 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. In this regard, it is important to consider the cyber-attacks as a risk challenging the integrity of critical infrastructures in a country including that used in key sectors such as energy, transportation, finance, and even the food supply chain.

- 2.5 While most countries in the LAC Region have organized and are operating Computer Security Incident Response Teams (CSIRT) according to a recent study published by the OAS<sup>4</sup>, 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 the national level; (ii) capacity building and training experts; 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 The respective project teams for the proposed TC and the TC *Setting the Ground for a Secure Cyber-Environment* (ATN/OC-14143/RG), which is commencing its implementation, will work to ensure complementarity between the two initiatives. The framework for CIP focuses on ensuring the protection of critical infrastructures and protection measures that go beyond addressing cyber threats, whereas the framework for cyber security is a horizontal framework aiming to address the overall level of cyber security within the society. Critical Infrastructure Protection and cyber security are generally subject to different legislative regimes, especially in those countries that have advanced the most in these areas.
- 2.9 **Objectives of the project.** The objectives of the TC are to contribute to the development and strengthening of CIP plans relevant to countries in the LAC Region by surveying and analyzing the best practices of other nations and regions and to make recommendations for the seamless, practical implementation of the plan.

---

<sup>2</sup> 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.

<sup>3</sup> VxWorks is a Real-Time Operation System (RTOS) developed by Windriver Systems. The system is often used for a spaceship or an aircraft.

<sup>4</sup> Latin American and Caribbean Cybersecurity Trends and Government Responses.

### 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 identified clusters of countries in the LAC region 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 and regions that are exemplary in the field, such as EU (e.g., European Program for Critical Infrastructure Protection), Korea (e.g., Guidelines on Critical 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. In this regard as part of the CT an effort will be made to group LAC countries in clusters, recommending specific actions depending upon the different status quo that each cluster (countries) is facing.
- 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.
- 3.4 **Component 2 – Conduct survey and analysis of the current status of CIP of LAC countries that are aggressively seeking ICT development and build regional capacity.** The objective of the component is to diagnose and analyze the status of CIP in at least one of the countries included in each identified cluster in the LAC Region, thereby producing inputs for the development of the next two components. The scope of the survey will cover laws, the organizational structure responsible for promoting cyber security as well as ICT, technological readiness, human capacity and so on.
- 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 for the different

- clusters identified. 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 systems 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 a roadmap to execute the recommendations that are identified during the project. Dissemination will consist of a publication and an event to present the results with the participation of ideally at least one representative from each of the countries of the LAC Region, including experts who would present international best practices.
- 3.8 **Expected results:** This project will enable a diagnosis of the current status and level of critical infrastructure protection in a group of representative 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
Study on best practice cases of lessons learned from leading countries in CIP	0	1 Study identifying best practices and main points of critical infrastructure protection plans and its roadmap in selected leading countries
Survey and analysis of current CIP status of countries in the LAC region	0	1 Comparative diagnosis of CIP status across the different clusters identified for the entire LAC Region.

Suggested Indicator(Outcome)	Base Line	Target at the end of the TC
organized by clusters		
Recommendations for laws and governance models for the institutions dealing with CIP	0	1 Report with set of recommendations, laws and other institutional suggestions for a successful CIP strategy among the identified clusters
Recommendation on technological aspects related to CIP in the identified clusters	0	1 Report with recommendations from the technological stand point including specific references to set up of CSIRT.
Workshop to discuss the results and present the major trends on cybersecurity with the participation of worldwide experts	0	1 - Workshop to present the major findings from the studies and the roadmap for the implementation of the recommendations identified for the different clusters

**Table 3.2: Indicative Budget (Unit: US\$)**

Component	Funding Sources		Total
	IDB	Korea	
Component 1: Research on the best practices	120,000	100,000	220,000
Component 2: Survey and analysis of CIP status of LAC countries by cluster	180,000		180,000
Component 3: Recommendations for laws and Institutions by cluster	140,000		140,000
Component 4: Recommendation for technological requirements by cluster	90,000	30,000	120,000
Component 5: Dissemination	10,000		10,000
<b>Total</b>	<b>540,000</b>	<b>130,000</b>	<b>670,000</b>

#### IV. EXECUTING AGENCY AND EXECUTING STRUCTURE

- 4.1 Considering that the project is to be implemented at a 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 provide an in-kind contribution to the project. In addition, to guarantee coordination and the suitability of the proposed recommendations, a steering committee will be created with the participation of representatives of the project team, the consulting firm, and the Republic of Korea, as strategic advisor. Moreover, this committee will invite the IDB borrowing member countries to participate throughout the execution. The selection and contracting of the individual consultants will be performed according to the processing guidelines from Human Resources for Complementary Workforce (AM-650); for the selection and contracting of consultancy firms and other consultancy services, the IDB Corporate Procurement Policy will apply (GN-2303-20).

## **V. PROJECT RISKS AND ISSUES**

- 5.1 **Difficulty in collecting data from countries via survey.** Gathering of survey data from the selected countries in each cluster may be challenging since each country may consider the result of the 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 in accordance with each countries' ICT development level. In particular, the technical cooperation will take into account that the set of recommendations should be adjusted to the reality of the respective clusters identified and in addition identify the ways in which the different countries should interact to guarantee a common understanding on how to handle, on a regional basis, the risks associated with cyber-attacks.

## **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](#))

**ANNEXES:**

- Annex I – Terms of Reference ([IDBDocs#38928961](#))
- Annex II – Procurement Plan ([IDBDocs#38928962](#))



**DEVELOPMENT OF CRITICAL INFRASTRUCTURE PROTECTION (CIP) PLAN  
AGAINST CYBER-ATTACKS**

**RG-T2458**

**CERTIFICATION**

I hereby certify that this operation was approved for financing under the Knowledge Partnership Korean Fund for Technology and Innovation (KPK) through a communication dated June 11, 2014 and signed by Mr. Suyeong Yu, Director of the International Bureau, Ministry of Strategy and Finance of the Republic of Korea. Also, I certify that resources from said fund are available for up to US\$540,000 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 from the funding source. 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.

(Original Signed)

08/12/2014

\_\_\_\_\_  
Sonia M. Rivera  
Chief  
Grants and Co-financing Management Unit  
ORP/GCM

\_\_\_\_\_  
Date

**APPROVAL**

Approved:

(Original Signed)

08/13/2014

\_\_\_\_\_  
Carlos Santiso  
Division Chief  
Institutional Capacity of the State Division  
IFD/ICS

\_\_\_\_\_  
Date