

## TECHNICAL COOPERATION DOCUMENT

### I. BASIC INFORMATION FOR TC

Country/Region:	Regional
TC Name:	Implementation of Critical Infrastructure Protection (CIP) Plan as a mean to strengthen the integrity and robustness of infrastructure
TC Number:	RG-T2698
Team Leader/Members:	Antonio Garcia Zaballos, Team Leader (IFD/CMF); Inkyung Jeun, Alternate Team Leader (IFD/CMF); Miguel Porrua (IFD/ICS); Kevin McTigue (LEG/SGO); Enrique Iglesias (IFD/CMF); Reinaldo Fioravanti (INE/TSP); Enrique Rodriguez (INE/ENE) and Cecilia Bernedo (IFD/CMF).
TC Taxonomy:	Client support (CS)
Date of TC Abstract authorization:	November 23, 2015
Beneficiary:	Chile and Bolivia
Executing Agency and contact name:	Inter-American Development Bank, Antonio García ( <a href="mailto:antoniogar@iadb.org">antoniogar@iadb.org</a> )
Donors providing funding:	Knowledge Partnership Korea Fund for Technology and Innovation (KPK)
IDB funding requested:	US\$650,000
Local counterpart funding:	US\$90,000 in kind contribution from the Republic of Korea
Disbursement period:	24 months (Execution period: 20 months)
Required start date:	March, 2016
Types of consultants:	Firm and individual consultants
Prepared by Unit:	Division of Capital Markets and Financial Institutions (IFD/CMF)
Unit of Disbursement Responsibility:	Institutions for Development Sector Department (IFD)
TC included in Country Strategy:	N/A
TC included in CPD:	
GCI-9 Sector Priority:	Institutions for Growth and Social Welfare

### 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%).

---

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

- 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, 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) which controls 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<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 see the cyber-attacks as a risk challenging the integrity of the critical infrastructure such as energy, finance, etc.
- 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

---

<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, 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.

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) creating 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. Toward this end, in 2014 the Inter-American Development Bank (IDB) approved a technical cooperation (RG-T2458; ATN/KK-14579-RG) with funding from the Republic of Korea to understand the current CIP status of each country in the LAC region to through surveys of relevant public and private stakeholders across various sectors and to establish a CIP plan.
- 2.8 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 Sector Strategy). Consistent with this 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
- 2.9 **Objective of the project.** The general goal of this Technical Cooperation (TC) is to support the governments of Chile and Bolivia in the implementation of a practical Critical Infrastructure Protection (CIP) framework for safe operation and protection of critical infrastructure. The CIP best practice developed through the TC RG-T2458 will be used as a recommendation for how to build a legal and organizational foundation for implementation.

### III. DESCRIPTION OF ACTIVITIES, COMPONENTS AND BUDGET

- 3.1 The activities proposed in this project are divided into four components to be implemented in two countries.<sup>5</sup> Component 1 includes current status of CIs in the countries and recommendations of necessary investments of systems and technologies (Hardware (HW) and Software (SW)), Component 2 includes analysis and further development of CIP governance frameworks, national awareness and capacity building programs, and Component 3 involves development of a roadmap for the establishment of CSIRT implementation and training. Finally, Component 4 consists of the financial analysis of proposed investments and operating costs.
- 3.2 **Component 1: Analysis of status quo, recommendations on systems and technology investments (HW and SW) for development.** The objective of this component is to identify, recommend, and design technical specifications for CIP systems in order to prevent and response to cyber incidents toward critical infrastructure. This component includes the following activities:

---

<sup>5</sup> The countries will be Chile and Bolivia and selection is based on the analysis undertaken from TC RG-T2458.

- (i) Identify and designate CIs among infrastructures for each country. Infrastructures whose extended incapacity or destruction would have a debilitating impact on national security, economic, public health and social safety should be designated as the critical infrastructures (e.g., telecommunication network, energy grid, banking system, etc.).
- (ii) Analyze threats and vulnerabilities on designated critical infrastructure systems. The scope of the vulnerability analysis will cover managerial (e.g. vulnerability in information security policy formulation and management, awareness and education), physical (e.g. Improper access control), and technological vulnerabilities (e.g. unauthorized access to critical infrastructure systems, delays in services and service failures). Penetration tests shall be used to look for security weaknesses and potential threats on the system.
- (iii) Design CIP measures to strengthen each of the critical infrastructure identified based on the previous vulnerability assessment. The security systems and managerial process will be identified and suggested considering the existing critical infrastructure environment.
- (iv) Recommend technology investments to support further prevention, detection, response capabilities of the government.

**3.3 Component 2: Development of CIP governance, national awareness and capacity building programs.** The objective of this component is to propose CIP-related laws, regulations and guidelines. This component includes the following activities:

- (i) Review and analysis of the existing regulatory environment associated with protection of critical infrastructures, information, and national security.
- (ii) Propose new or modify CIP-related legislation in relation to meet CIP best practices. This legal framework will cover the obligation and authority for CIP activities, roles of stakeholders, and organization structure of supervisory agency.
- (iii) Develop processes for information sharing of incidents between CIP stakeholders.
- (iv) Advise on the national CIP promotion, awareness and capacity building agendas to create cyber savvy citizens, and recommend ways to further strengthen and extend government alliances with public and private sector parties, both national and international.

**3.4 Component 3 –Design roadmap for CIP implementation and support the establishment of a Critical Infrastructure Incidents Response organization.** The objective of this component is to prepare a roadmap for the establishment of a national Computer Security Incidents Response Team (CSIRT) to response to cyber incidents on CI and establish response strategies. This component includes the following activities:

- (i) Create a roadmap and CSIRT project schedule for deployment of technology and services, expanding on stages for detailed design and engineering, construction, operations, service introduction, monitoring, etc.
- (ii) Identify key personnel for management, maintenance and operations of the CSIRT, and commercial and operational alternatives including ownership structure, management mechanisms and options for operations and maintenance.
- (v) Training of identified CSIRT members to prevent, detect, and respond to cyber or physical incidents. It includes incident investigation of malicious codes, network and system log analysis, etc.

**3.5 Component 4: Conduct financial analysis on the deployment and operation of proposed technological investments and creation of CSIRT.** Based on the findings of the previous section, the goal of this component is evaluate the financial aspects and its respective business model. This component includes the following activities:

- (i) Evaluate the investments, analyze the economic rate of return and cost benefit analysis associated with the proposed investments. Must include CAPEX/OPEX and ROI models associated with the investment and human resources, which implies an estimation of the expected demand for services; the operative break-even point, defined as the minimum investment that make the deployment economically viable; and of the savings associated with the services as compared to the current situation.
- (ii) Propose appropriate Business and Public Private Partnership (PPP) models based on CIP best practices.

**3.6 Expected results.** The expected results of this project consists of establishment of a CIP governance framework consisting of new legislation, development of national promotion and awareness agenda and increased capacity to prevent, detect, and address physical and cyber-attacks. Ultimately, it will contribute to enhancing national security through strengthening of national critical infrastructure.

**Table 1: Indicative Results Matrix**

Suggested Indicator(Outcome)	Measurement Unit	Base Line	Target at the end of the TC
Component 1: Analysis of status quo, recommendations on systems and technology investments (HW & SW). <ul style="list-style-type: none"> <li>Identify and designate Critical Infrastructures.</li> <li>Analyze threats and vulnerabilities on designated critical infrastructure systems.</li> <li>Design CIP measures to strengthen each of the critical infrastructures.</li> <li>Recommend technology investments.</li> </ul>	No. of Documen	0	2
Component 2: Development of CIP governance framework, national awareness and capacity building programs. <ul style="list-style-type: none"> <li>Review and analysis of existing regulatory.</li> </ul>	No. of Documen	0	2

Suggested Indicator(Outcome)	Measurement Unit	Base Line	Target at the end of the TC
<ul style="list-style-type: none"> <li>Propose new or modify CIP legislation.</li> <li>Develop processes for information sharing of incidents.</li> <li>Advise on the national CIP promotion, awareness and capacity building agendas.</li> </ul>			
Component 3: Design roadmap for CIP implementation and support the establishment of a CI incidents response organization. <ul style="list-style-type: none"> <li>Create a roadmap and CSIRT project schedule for deployment.</li> <li>Identify key personnel for management, maintenance and operations of the CSIRT.</li> </ul>	No. of Documents	0	2
Component 4: Conduct financial analysis on the deployment and operation of proposed technological investments and creation of CSIRT. <ul style="list-style-type: none"> <li>Evaluate the investments, and analyze the economic rate of return.</li> <li>Propose appropriate business and PPP models.</li> </ul>	No. of Documents	0	2
Trainings for Computer Security Incidents Response Team.	No. of Trainings	0	2

3.7 The estimated total cost of this Technical Cooperation is US\$740,000, of which US\$650,000 will be financed by the Knowledge Partnership Korea Fund for Technology and Innovation (KPK), and US\$90,000 will be provided by the Republic of Korea as an in-kind contribution.

**Table 2: Indicative Budget (US\$)**

Components	Funding Sources		Total
	IDB (KPK)	Republic of Korea	
Component 1: Analysis of status quo, recommendations on systems and technology investments (HW & SW).	245,000	50,000	295,000
Component 2: Development of CIP governance framework, national awareness and capacity building programs.	130,000	-	130,000
Component 3: Design roadmap for CIP implementation and support the establishment of a CI incidents response organization.	120,000	40,000	160,000
Component 4: Conduct financial analysis on the deployment and operation of proposed technological investments and creation of CSIRT.	130,000	-	130,000
Dissemination.	25,000	-	25,000
<b>Total</b>	<b>650,000</b>	<b>90,000</b>	<b>740,000</b>

#### IV. EXECUTING AGENCY AND EXECUTING STRUCTURE

4.1 Considering that the project implies the involvement of institutions from the different strategic sectors in Chile and Bolivia and the need of establishing a dialogue and a

clear coordination in the definition of the regulatory framework and the policies related to the roadmap for a CIP strategy, and taking into account the request from the Governments of Chile and Bolivia, the executing agency will be the Bank through the IFD/CMF Division, which has broad experience working with the indicated institutions. Prior to the initiation of activities in the Beneficiary Country of the Plurinational State of Bolivia, a non-objection letter will be sought from the country liaison entity with the Bank.

- 4.2 The Bank will contract individual consultants, consulting firms and non-consulting services in accordance with Bank's current procurement policies and procedures.
- 4.3 The coordination and monitoring within every country will be done through the Ministries of Transport and Telecommunications that will coordinate the participation of the institutions responsible for the regulation and development of public policies related to critical infrastructure.

## **V. MAJOR ISSUES**

- 5.1 **Difficulty in collecting information about critical infrastructure from countries.** Gathering of information from countries may be challenging since each country may consider the information about critical infrastructure is important and confidential, thus, be reluctant to share this information. Therefore, an elaborate, inclusive communication strategy is required to encourage countries' understandings and involvement in the project. In addition we will create a steering and a technical committee to make sure that the institutions are involved and informed about the work done, this will facilitate the information gathering, the information analysis and the specific recommendations which could eventually come out of such an analysis.

## **VI. EXCEPTIONS TO THE BANK POLICY**

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

## **VII. ENVIRONMENTAL AND SOCIAL STRATEGY**

- 7.1 The nature of the TC that includes a roadmap for a critical infrastructure protection strategy expects no environmental and social risks associated with it. This operation is classified as a Category "C" according to the Environment and Safeguards Compliance Policy (OP-703) (see [Safeguard Policy Filter Report and Safeguard Screening Form](#)).

### **REQUIRED ANNEXES:**

- Annex I: [Request Letters](#)
- Annex II: [Terms of Reference \(ToR\)](#)
- Annex III: [Procurement Plan](#)


IMPLEMENTATION OF CRITICAL INFRASTRUCTURE PROTECTION (CIP) PLAN AS A MEAN TO STRENGTHEN THE  
INTEGRITY AND ROBUSTNESS OF INFRASTRUCTURE

RG-T2698

CERTIFICATION

I hereby certify that this operation was approved for financing under the Knowledge Partnership Korea Fund for Technology and Innovation (KPK), through a communication dated November 23, 2015 and signed by Chang Yeon You. Also, I certify that resources from said fund are available for up to US\$650,000 in order to finance the activities described and budgeted in this document. This certification reserves resource 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, i.e. represent a risk that will not be absorbed by the Fund.

H.M.S

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

03/14/2016  
Date

Approved:

  
\_\_\_\_\_

Juan Antonio Ketterer  
Division Chief  
Capital Markets and Financial Institutions  
IFD/CMF

03/14/2016  
Date