TECHNICAL COOPERATION ABSTRACT

I. BASIC INFORMATION

Country:	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); Kevin McTigue (LEG/SGO); Enrique Iglesias (IFD/CMF); and Cecilia Bernedo (IFD/CMF).
TC Taxonomy:	Research and Development (RD)
Authorization TC date:	August, 2015
Beneficiary:	Latin American and Caribbean Region (LAC)
Executing agency and contact name:	Inter-American Development Bank, Antonio García (antoniogar@iadb.org)
Donors providing funding:	Knowledge Partnership Korea Fund for Technology and Innovation (KPK)
IDB funding requested:	US$650,000
Local counterpart funding:	US$90,000 Republic of Korea (in kind)
Disbursement period:	24 months (Execution period: 20 months)
Required start date:	September, 2015
Types of consultants:	Firm and individual consultants
Prepared by Unit:	Division of Capital Markets and Financial Institutions (IFD/CMF)
Unit of disbursement responsibilit	Institutions for Development Sector Department (IFD)
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)[1], the number of the Internet users in the LAC Region amounts to 254.91 million or 10.4% in the world. From 2000 to

[1] http://www.internetworldstats.com/.

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[2] and VxWorks[3] 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] 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.

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

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[4], 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) 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 Republic of Korea to understand the current CIP status of each country in the LAC region though surveys of relevant public and private stakeholders across various sectors and establish a CIP plan.

2.8 **Objective of the project.** The general goal of this Technical Cooperation (TC) is to support the government of the Region in the implementation of a practical Critical Infrastructure Protection (CIP) framework for safe operation and protection of critical infrastructure. CIP best practice developed through previous operation ATN/KK-14579-RG (Development of Critical Infrastructure Protection Plan against Cyber-Attacks), will be used as a recommendation for how to build a legal and organizational foundation for implementation.

III. DESCRIPTION OF ACTIVITIES

3.1 The activities proposed in this project are divided into four components to be implemented for two countries[5]. 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.

[4] Latin American and Caribbean Cybersecurity Trends and Government Responses

[5] The countries shall be selected among countries that have a plan to develop a CIP-related strategy and understand the importance of the CIP based on the findings from TC ATN/KK-14579-RG.

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:

(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 3.1: 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). • Identify and designate Critical Infrastructures. • Analyze threats and vulnerabilities on designated critical infrastructure systems. • Design CIP measures to strengthen each of the critical infrastructures. • Recommend technology investments.	No. of Document	0	2
Component 2: Development of CIP governance framework, national awareness and capacity building programs. • Review and analysis of existing regulatory. • Propose new or modify CIP legislation. • Develop processes for information sharing of incidents. • Advise on the national CIP promotion, awareness and capacity building agendas.	No. of Document	0	2
Component 3: Design roadmap for CIP implementation and support the establishment of a CI incidents response organization. • Create a roadmap and CSIRT project schedule for deployment. • Identify key personnel for management, maintenance and operations of the CSIRT.	No. of Document	0	2
Component 4: Conduct financial analysis on the deployment and operation of proposed technological investments and creation of CSIRT. • Evaluate the investments, and analyze the economic rate of return. • Propose appropriate business and PPP models.	No. of Document	0	2
Trainings for Computer Security Incidents Response Team.	No. of Trainings	0	2

Table 3.2: Indicative Budget (Unit: US$)

Components	Funding Sources		Total
	IDB	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
Total	**650,000**	**90,000**	**740,000**

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/CMF Division, which has broad experience working with the indicated institutions. IFD/CMF will operate in coordination with the Republic of Korea, which will inject in-kind contribution into the project. In addition, to guarantee the coordination among the countries and the suitability of the proposed recommendation it will be created a steering committee with the participation of one representative from each countries as a focal point and as a part of a working group to provide guidelines throughout the execution.

4.2 The procurement of individual consulting services will be carried out by the IDB in accordance with Human Resources (HRD) policies (AM-650). The procurement of firm consulting services will be carried out by the IDB in accordance with the Policies for the Selection and Contracting of Consultants Financed by the Inter-American Development Bank (GN-2350-9). The procurement of consulting services different from consultants will be carried out by IDB in accordance with Corporate Procurement Policies (GN-2303-20) while IDB's new policies regarding the matter are not in force.

V. Project Risks and 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.

5.2 **Delay in the execution of the project due to lack of information and coordination**. Lack of information related to this topic, as well as elaborate coordination between involved entities could cause delays in the execution of the project. To mitigate this risk, the Team will have a close monitoring of the design, implementation and results obtained in each of the phases identified in the TC.

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. 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).