**REGIONAL**

**Development of Critical Infrastructure Protection (CIP) Plan as a Mean to Strengthen the Integrity and Robustness of Infrastructure**

**(RG-T2458)**

**Research on Best Practice Cases of Leading CIP Countries and Recommendations for Satisfaction of technological requirements for CIP**

**Terms Of Reference**

1. Background

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 Stats (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%).

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 that the incapacitation or destruction of which 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 up to 40% from 2011 to 2012 (Latin American and Caribbean Cybersecurity Trends and Government Responses, May 3, 2013).

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.

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 loomed 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]](#footnote-1) and VxWorks[[2]](#footnote-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.

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.

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 legislations at national level; (ii) nurturing professionals; and (iii) promoting public awareness.

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.

**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. 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

These terms of reference define the required background and expertise, as well as the objectives, activities, products and services to be delivered by a Consultant hired in the framework of the TC. Overall, the TC is designed to effectively support the development of a model critical infrastructure protection plan for adoption by countries in the LAC region.

1. Consultancy Objective

The main objectives of this consultancy are to conduct research on best practice cases of leading countries in critical infrastructure protection and to provide recommendations for the satisfaction of technological requirements to make a national CIP plan successful. 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

1. Characteristics of This Consultancy

Type of Consultancy: Individual

**Start date and duration:** from July, 2014 to Dec, 2015. **Estimated duration period:** 18 months.

**Place of work/travel:** Place of residence. Travel required. During the period, the individual is expected to make one site-visit for research of best practice and another site-visit for training of government officials from LAC countries.

**Qualifications:** The consultant must have an extensive experience and high-level understanding of issues pertaining to national critical infrastructure protection (CIP), ranging from policies and regulations to technologies required for the establishment of a national Computer Security Incident Response Team. Since the focus of the research is on identifying the most suitable practices among best practice cases of leading countries in CIP for the LAC region, the experience of planning and international cooperation will be highly weighed. The consultant must have effective presentation and communication skills to facilitate understanding of government officials of LAC countries about research outcome. Considering the important role of government in formulating and implementing a CIP plan and the provision of funding by the government of Korea, the consultant with experience in working with government counterparts would be valued.

**Source of funding:** RG-T2458

**IV. Description of Activities**

The activities to be implemented within these components are to conduct research on best practice cases of leading CIP countries and to provide recommendations for the satisfaction of technological requirements for CIP in order to identify the most suitable practice for countries in the LAC Region. 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

**Activity 1: Survey and analysis of best practice cases**The consultant will research and analyze at least three best practice cases currently being implemented in countries that are exemplary in the field, such as EU, Korea and Israel. In addition, the consultant will make the result of analysis available on the website, including national and regional CIP policies, relevant laws and regulations, practices and principles and challenges, which will serve as guidelines for countries in the LAC region.

**Activity 2: Site-visit training**The consultant will arrange a workshop with training opportunities in order to facilitate sharing the latest updates and reaching a consensus on adopting a best practice at regional level. This event will take place in one of the leading countries in the field, inviting government officials from around ten LAC countries.

**Activity 3: Recommending technological measures to support effective prevention, detection and counteraction**In order to facilitate understanding of how a CIP plan is translated into performance, the consultant will provide the best practice cases of national Computer Security Incidents Response Teams (CSIRT) and make recommendations on the procedures and methods for the establishment of CSIRT. For example, the consultant will provide the historical background of Korea Internet Incident Center (KISC) established within Korea Internet and Security Agency (KISA) and discuss ways to legally collect traffic information from privately owned and operated telecommunication service providers. Also, the consultant will explain the basic requirements for technical equipment being used at KISC.

**V. Products**

Product A: Key points of a successful CIP plan and its implementation activities for the LAC region based on the analysis of at least three best practice cases of exemplary countries

Product B: Workshop with training opportunity for government officials of LAC countries for sharing information and building consensus

Product C: Methods for developing technological preparedness including the procedure of setting up and advancing CSIRT

**Vi. Method of Payment**

Payments shall be made as per the following schedule, upon approval by the Team Leader responsible for this TC (See item VII below).

Schedule of payments:

* + 1. 30 % upon signing the contract
    2. 40 % upon getting approval on product A
    3. 30 % upon completing product B and getting approval on product C

**VII. Coordination**

Supervision and coordination of the firm’s work will be the responsibility of Antonio García Zaballos (IFD/CTI), Team Leader, antoniogar@iadb.org, Telephone (202) 623-2980.

**REGIONAL**

**Development of Critical Infrastructure Protection (CIP) Plan as a Mean to Strengthen the Integrity and Robustness of Infrastructure**

**(RG-T2458)**

**Survey and Analysis of Current Status of CIP in**

**Selected Countries in LAC Region**

**Terms Of Reference**

**I. Background**

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 Stats (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%).

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 that the incapacitation or destruction of which 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 up to 40% from 2011 to 2012 (Latin American and Caribbean Cybersecurity Trends and Government Responses, May 3, 2013).

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.

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 loomed 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[[3]](#footnote-3) and VxWorks[[4]](#footnote-4) 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.

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.

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 legislations at national level; (ii) nurturing professionals; and (iii) promoting public awareness.

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.

**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. 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

These terms of reference define the required background and expertise, as well as the objectives, activities, products and services to be delivered by a Consultant hired in the framework of the TC. Overall, the TC is designed to effectively support the development of a model critical infrastructure protection plan for adoption by countries in the LAC region.

**II. Consultancy Objective**

The main objectives of this consultancy are to conduct survey and analysis of the current status of CIP of LAC countries such as Brazil, Argentina, Costa Rica, etc. that are aggressively seeking ICT development and building regional capacity.

**III. Characteristics of This Consultancy**

**Type of Consultancy:** Firm

**Start date and duration:** from July, 2014 to February, 2016. **Estimated duration period:** months.

**Place of work/travel:** Place of residence. Travel required. During the period, the consulting firm is expected to make one or more site-visit(s) for survey and one or more site-visit(s) for sharing the result of survey with and training of government officials from LAC countries.

**Qualifications:** The consulting firm must have within the firm: a senior member and a policy/legal expert in ICT laws and regulations with extensive professional experience in ICT projects in developing countries. Experience in Latin American countries will be highly weighed. The consulting firm must have effective presentation and communication skills to facilitate understanding of government officials of LAC countries about survey outcome. Considering the important role of government in formulating and implementing a CIP plan and the provision of funding by the government of Korea, the consulting firm with experience in working with government counterparts would be valued.

**Source of funding:** RG-T2458

**IV. Description of Activities**

The activities to be implemented within these components are to conduct survey and analysis of the current status of CIP of selected countries in the LAC region, the result of which will form the basis of the next component – provision of recommendations for legal and institutional developments and guidelines. 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.

**Activity 1: Survey and analysis of current laws, policies and technical measures employed for CIP**The consulting firm will diagnose and analyze the status of CIP in countries in the LAC region. To this end, the consulting firm will develop criteria for the selection of countries and for the categorization of the level of ICT development and recognition of the significant implication of CIP. Also, the consulting firm will design in such a way to produce meaningful information on key areas, such as laws, policies, technical measures, practices and principles, structure of organizations in charge of CIP and ICT, technical readiness, human capacity, etc., to enable objective comparison and contrast among countries.   
Since the result of this activity will be the foundational input to the development of recommendations for CIP-related laws and institutions as well as a set of regional guidelines, which is expected to be carried out by another consultant, an alignment needs to exist between the two consulting parties. Therefore, the consulting firm will involve the consultant in the designing phase of survey questions expected outcomes and provide consultation so requested by the consultant about the result of survey during and after the completion of this activity.

**Activity 2: Regional workshop(s) and local off-site training session(s)**The consulting firm will organize, in association with a regional dialogue, regional workshop(s) and local off-site training session(s) in order to share the outcome of this survey and analysis with government officials of countries in the LAC region.

**Activity 3: Provide master plan for CIP consisting of laws, policies, organizational structure and institutional capacity building**Based on the results from the analysis of best practice cases of leading CIP countries and the survey of the current status of CIP in selected countries in the LAC region, the consultant will provide recommendations for laws, guidelines and programs tailored for the LAC region. With respected to institutional capacity building, the consultant will suggest appropriate steps towards establishing and operating CIP system in public sector and an inter-governmental organizational model required to promote effective and responsive coordination among relevant government bodies.

**V. Products**

Product A: Rationally categorized status of CIP in selected countries in the LAC region which allows for objective comparison

Product B: Workshop(s) and training session(s) for government officials of LAC countries to share survey outcome

Product C: Set of recommendations for laws and policies and institutional suggestions for CIP for adoption by countries in the LAC region

**Vi. Method of Payment**

Payments shall be made as per the following schedule, upon approval by the Team Leader responsible for this TC (See item VII below).

**Schedule of payments:**

30 % upon signing the contract;

40 % upon approval of Product A and completion of Product B;

30% upon approval of Product C

**VII. Coordination**

Supervision and coordination of the firm’s work will be the responsibility of Antonio García Zaballos (IFD/CTI), Team Leader, antoniogar@iadb.org, Telephone (202) 623-2980.

**REGIONAL**

**Development of Critical Infrastructure Protection (CIP) Plan as a Mean to Strengthen the Integrity and Robustness of Infrastructure**

**(RG-T2458)**

**Recommendations for Laws, Policies and Institutions for CIP**

**Terms Of Reference**

**I. Background**

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 Stats (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%).

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 that the incapacitation or destruction of which 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 up to 40% from 2011 to 2012 (Latin American and Caribbean Cybersecurity Trends and Government Responses, May 3, 2013).

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.

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 loomed 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[[5]](#footnote-5) and VxWorks[[6]](#footnote-6) 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.

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.

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 legislations at national level; (ii) nurturing professionals; and (iii) promoting public awareness.

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.

**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.

1.9 These terms of reference define the required background and expertise, as well as the objectives, activities, products and services to be delivered by a Consultant hired in the framework of the TC. Overall, the TC is designed to effectively support the development of a model critical infrastructure protection plan for adoption by countries in the LAC region.

**II. Consultancy Objective**

The main objective of this consultancy is to develop and provide recommendations for the procedures and elements of CIP-related laws and a set of guidelines for countries in the LAC region. 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

**III. Characteristics of This Consultancy**

**Type of Consultancy:** Individual

**Start date and duration:** from October, 2014 to February, 2016. **Estimated duration period:** 17 months.

**Place of work/travel:** Place of residence. Travel required. During the period, the consultant is expected to participate in coordination meetings with IDB specialists at Headquarters (Washington, DC).

**Qualifications:** The consultant must have extensive experience in ICT and CIP, ranging from policy and regulation to technologies. In addition, The experience in planning and international cooperation will be highly weighed. The consultant must also have capacity to facilitate collaboration with other consultants. Considering the important role of government in formulating and implementing a CIP plan and the provision of funding by the government of Korea, the consultant with experience in public sector and/or working with government counterparts as well as the knowledge of laws would be valued.

**Source of funding:** RG-T2458

**VI. Description of Activities**

The activities to be implemented within this component to develop and recommend procedures and elements of CIP-related laws and a set of regional guidelines. 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

**Activity 1: Provide master plan for CIP consisting of laws, policies, organizational structure and institutional capacity building**Based on the results from the analysis of best practice cases of leading CIP countries and the survey of the current status of CIP in selected countries in the LAC region, the consultant will provide recommendations for laws, guidelines and programs tailored for the LAC region. With respected to institutional capacity building, the consultant will suggest appropriate steps towards establishing and operating CIP system in public sector and an inter-governmental organizational model required to promote effective and responsive coordination among relevant government bodies.

**V. Products**

Product A: Set of recommendations for laws and policies and institutional suggestions for CIP for adoption by countries in the LAC region

**Vi. Method of Payment**

Payments shall be made as per the following schedule, upon approval by the Team Leader responsible for this TC (See item VII below).

Schedule of payments:

* + 1. 30 % upon signing the contract;
    2. 20 % upon intermediary approval of the progress report for developing Product A;
    3. 50 % upon approval of Product A

**VII. Coordination**

Supervision and coordination of the firm’s work will be the responsibility of Antonio García Zaballos (IFD/CTI), Team Leader, antoniogar@iadb.org, Telephone (202) 623-2980.

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. [↑](#footnote-ref-1)
2. VxWorks is a Real-Time Operation System (RTOS) developed by Windriver Systems. The system is often used for a spaceship or an aircraft. [↑](#footnote-ref-2)
3. 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. [↑](#footnote-ref-3)
4. VxWorks is a Real-Time Operation System (RTOS) developed by Windriver Systems. The system is often used for a spaceship or an aircraft. [↑](#footnote-ref-4)
5. 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. [↑](#footnote-ref-5)
6. VxWorks is a Real-Time Operation System (RTOS) developed by Windriver Systems. The system is often used for a spaceship or an aircraft. [↑](#footnote-ref-6)