TECHNICAL COOPERATION TC - ABSTRACT

PARAGUAY

I. BACKGROUND

Country:	Paraguay		
TC Name:	Diagnosis and development of broadband and cyber-security plans		
TC Number:	PR-T1151		
Team Leader/Members:	Miguel Porrua (IFD/ICS), Team Leader; Pablo Angelelli (IFD/CTI); Felix Gonzalez Herran (IFD/CTI); Nathalia Foditsch (IFD/CTI); Enrique Iglesias (IFD/CTI); Cecilia Bernedo (IFD/CTI) and Carmen Masters, (IFD/CTI)		
TC Taxonomy:	Client Support (CS)		
Reference to request:	IDBDocs#37785044		
Date of TC Abstract authorization:	To be determined (TBD)		
Donors providing funding:	TBD		
Beneficiary:	Paraguay		
Executing agency and contact name:	Viceministry of Telecommunications		
IDB Funding Requested:	IDB:		US$500,000
Local counterpart funding:	Local:		US$ 0
	Total:		US$500,000
Execution period:	18 months	**Disbursement period:**	21 months
Required start date:	July, 2013		
Types of consultants:	Firm and individual consultants		
Prepared by Unit:	Division of Competitiveness, Technology and Innovation (IFD/CTI)		
Unit of Disbursement Responsibility:	IFD/CTI		
TC included in Country Strategy:	N/A	**TC included in CPD:**	N/A
GCI-9 sector priority:	Mentioned under current sector strategies: "Support Competitive Global and Regional Integration", and "Institutions for Growth and Social Welfare".		

II. OBJECTIVES AND JUSTIFICATION OF THIS TC

2.1 There is evidence that the acceleration of broadband penetration, adoption and effective use brings clear social and economic benefits. In particular, it is estimated that increases of 10% in broadband penetration in Latin American and

Caribbean (LAC) countries, on average, have associated increases of 3.19% in GDP, 2.61% in productivity and a net generation of more than 67,000 jobs[1].

2.2 Paraguay is one the countries in the LAC region that faces challenges to effectively harness the benefits brought about by broadband connectivity, as it is characterized by: (i) low levels of penetration, with only 5.43 lines per 100 inhabitants adding both fixed and mobile broadband penetration[2] versus an average of 6,24 lines per 100 inhabitants in LAC countries and 32 lines per 100 inhabitants in OECD countries[3]; (ii) low broadband quality, in terms of speed, averaging approximately 1.8 Mbps for fixed broadband versus 3.7 Mbps in LAC and 19.9Mbps in OECD countries[4]: and (iii) very high prices, where the average plan costs nearly US$60 PPP per Mbps, while the average cost for LAC and OECD countries is US$53.17 and US$7.26 PPP per Mbps[5] respectively.

2.3 In this line, the main barriers found in Paraguay to increase broadband penetration, adoption and use are: (i) limited awareness of the benefits that broadband and ICTs have particularly regarding their potential for innovation and competitiveness in sectors such as health, education, government, trade, finance and SMEs, as well as a general lack of skills for their adoption by public officials, policy makers, entrepreneurs and citizens; (ii) insufficient institutional capacity and lack of a governance model to design, implement and monitor specific policies promoting the adoption and effective use of ICTs for all the population; (iii) outdated regulatory frameworks that fail to adequately attend the recent evolution of the telecommunications sector; (iv) inadequate deployment of infrastructure and technology; and (v) lack of reliable, measurable and updatable data to monitor and evaluate ICT policies, the regulatory situation, the level of infrastructure deployment and the prevalence of ICT applications and services.

2.4 On top that, Paraguay needs to be the ready, in terms of cyber-security, to an explosion in traffic thanks to the increasing deployment of broadband infrastructure. Indeed, a 2012 cyber-attack levied against the Paraguay's national energy utility raised questions of the resilience of the country's critical infrastructure.

2.5 The Government of Paraguay has recognized the importance of addressing these two challenges, one in broadband and one in cyber-security. As for the latter, it noteworthy that its importance has become greater in the past few years. Cyber-attacks in Paraguay and elsewhere have highlighted that secure networks are needed to ensure the uninterrupted provision of government services to citizens, promote economic and social development, maintain international competitiveness, and include citizens in the democratic process. For that reason, Paraguay launched its national Computer Security Incident Response Team (CSIRTpy) in late 2012, illustrating its will to invest in cyber security initiatives.

---

1 Garcia-Zaballos, A. / López-Rivas, R.: Governmental control on socio-economic impact of broadband in LAC countries. IDB, 2012.

2 ICT World Indicators Database, International Telecommunications Union (June, 2012).

3 Internal calculation out of ICT World Indicators Database, International Telecommunications Union (June, 2012).

4 Galperín, H.: Broadband prices and quality in Latin America (2012).

5 Ibid.

2.6 In light of the many challenges observed to promote broadband in Paraguay and the importance of tackling the cyber-security arena in present times, the Government requested technical and financial support from the Inter-American Development Bank (IDB) to address these issues through this technical cooperation.

2.7 **Objectives of the project:** The goal of this Technical Cooperation (TC) is to provide support to the Paraguayan Government in the process of promoting broadband universalization in terms of access, as well as to support them in cyber-security strategic policies and regulation, taking into account the efforts that the government is already making in both arenas.

III. DESCRIPTION OF ACTIVITIES

3.1 The activities proposed in this project are divided into four main components, which define its strategic approach. Component 1 includes a diagnostic and analysis of the supply and demand for broadband services in Paraguay and the infrastructure requirements to meet the existing access gap. This analysis will be crucial for the government to make proposals, primarily on connectivity for educational centers and health centers, to the FONACIDE fund (*Fondo Nacional de Inversión Pública y Desarrollo*). This component also comprises an assessment of the cyber security infrastructure, in terms of hardware and software. Component 2 proposes a cyber-security national plan and its corresponding governance model. It also comprises a review of existing national broadband plan. Component 3 reviews and proposes updates to the regulatory framework and legislation in order to promote the necessary investment and boost broadband development as well as cyber-security. Component 4 includes specific workshops and training sessions, one corresponding to each of the previous components.

3.2 **Component 1: Diagnostic and analysis of alternative infrastructure for broadband deployment and cyber security.** The objective of this component is to conduct a feasibility study to determine the required investments that will allow the government to move towards universal access and service of broadband; and the required investments in terms of cyber security infrastructure. The feasibility study on broadband connectivity will be essential for the government as an input to create proposals to the FONACIDE fund, with a particular focus on educational center and health centers. This activity includes:

(i) A diagnostic of the access gap in the country, specifically the gap between supply (considering backbone, backhaul and access networks) and demand and how this gap may be bridged through appropriate State policy with a focus on education and health centers.

(ii) Field-study to analyze the design of the necessary infrastructures to meet the estimated demand. This study will analyze the existing and planned infrastructure deployments as well as the estimated demand based on a survey study that will be complemented by a bottom-up model based on the geographic and socio-economic characterization of the country. The result will be an estimation of the costs associated with the necessary networks'

deployment per type of technology. The analysis will tackle the connectivity for education institutions (schools, universities, training centers), health institutions (hospitals, health centers), government facilities, households and any other dependency subject to be connected (e.g. private companies).

(iii) Analysis of the economic return associated with the different alternatives for deploying broadband networks (FTTx, HFC, WiMAX, 3G, among others), taking into account the different deployment scenarios (high-density urban areas, urban, and rural). An estimation of the Net Present Value (NPV) associated with the investment is required, which implies an estimation of the expected demand for services; the operative break-even point, defined as the minimum number of lines or the minimum service penetration that make the deployment economically viable; and of the price levels associated with the different types of services.

(iv) Assessment of the cyber-security infrastructure in Paraguay both in terms of software and hardware taking into account the traffic growth that could be the result of a broadband deployment. The technical assessment will be accompanied by a financial model where the CAPEX and OPEX will be identified.

3.3 **Component 2: Development of a national cyber-security plan and corresponding governance model; incorporating reviews of the existing national broadband plan and telecommunications regulatory framework.** The objective of this component is to support the design of a comprehensive cyber-security and cybercrime policy or plan that engages all relevant stakeholders and addresses the range of cyber-security challenges in a strategic and forward-looking manner. An additional objective will be to review the current national broadband plan and telecommunications regulatory framework, elaborating specific enhancements and updates where applicable. The cyber-security policy/strategy shall incorporate a regulatory/auditing regime. Ensuring adequate regulation for cyber-security infrastructures/policies, broadband, and telecommunications in general is central to the success of this project, since private sector investment in cyber and access infrastructures requires a stable and predictable regulatory frame work. The activities included in this component will be:

(i) Review of any existing cyber-security policies.

(ii) Review of the existing national broadband plan, proposing improvements and modifications or updates where applicable.

(iii) Review of the national telecommunications regulatory framework, particularly clauses on access, interconnectivity, and the radio-electric spectrum.

(iv) Review of existing cybercrime legislation and composition of an action plan and timeline for modernizing legislation, if necessary.

(v) Draft of a plan outlining Paraguayan cyber-security goals and priorities assessing the needs in terms of cyber-security infrastructure, especially regarding electronic commerce and banking and digital signature.

(vi) Outline and definition of mechanisms by to cooperate and share information both domestically and internationally; proposing improvements and modifications where applicable and updating the data.

(vii) Definition of roles and responsibilities of all key cyber-security stakeholders in Paraguay; including lead – and regulating – agencies.

(viii) Composition of an implementation chronogram with an estimated budget for achieving goals laid out in cyber-security plan, including specific action items.

3.4 **Component 3: Review of the regulatory framework for telecommunications and cyber-security.** The objective of this component is to review and propose updates to the regulatory framework and legislation in order to boost broadband and cyber-security development. As for the former, this component is particularly relevant as the decision of investing in the deployment of access infrastructures by the private sector requires a stable and predictable regulatory framework that creates the conditions to facilitate investments, thus promoting universality in access. As for the latter, specific cyber-security legislation is crucial for Paraguay to enhance country's capabilities to pursue and prosecute cyber-crime and set up the foundations that permit ICTs development in cutting-edge technologies such as e-commerce, e-banking and digital signature. This component includes the following activities:

(i) review (assessment and proposal for enhancements) of the telecommunications regulatory framework paying special attention to aspects associated with access, interconnection, radio-electric spectrum and universal service;

(ii) review (assessment and proposal for enhancements) of the cyber-security regulatory framework paying attention to aspects associated e-commerce, e-banking and digital signature; and

(iii) elaboration of a proposal to modify the existing legislation and to develop new and up to date legislation, defining the steps required for its implementation on the points outlined in section 3.3.i and 3.3.ii;

3.5 **Component 4: Workshops to disseminate results and to provide light cyber-security training.** The objective of this component will be to hold a workshop with key stakeholders after completing each of the Components 1, 2 and 3. The objective will not only to present the results but also to provide light technical training on incident response and cyber investigation for government officials and key private sector actors, including critical infrastructure owners and operators.

3.6 **Expected outputs:** In particular, the project will provide technical assistance to:

(i) Diagnostic of the connectivity gap between supply and demand;

(ii) Study to identify broadband infrastructure requirements in Paraguay and the economic return associated to its deployment, according to different technologies and geographic areas;

(iii) National Cyber-security Plan, including an action plan, governance model and an implementation chronogram with goals and an estimated budget;

(iv) Review of the existing National Broadband Plan; and

(v) Proposal to update specific legislation to improve the telecommunications and cyber-security regulatory framework.

3.7 **Expected results:** As a result of this project, the Government of Paraguay will have a better understanding of the current status of broadband and cyber-security in the country, as a necessary initial step to design appropriate policies and regulations aimed at accelerating broadband penetration, adoption and use in the country coupled with cyber-security infrastructure, policies and regulations. Ultimately, a greater penetration of broadband connectivity is expected to increase competitiveness and social inclusion, and facilitate greater economic interaction of Paraguay with external markets.

Table 3.1: Indicative matrix of the results

Suggested indicator	Measurement Unit	Baseline	Target at the end of the TC
Output Indicators:			
Component 1: - Diagnostic of the connectivity gap between supply and demand in Paraguay - Study to identify broadband infrastructure requirements in Paraguay and the economic return associated to its deployment - Study to identify cyber-security infrastructure requirements in Paraguay and its associated financial analysis	No. of Documents	0	3
Component 2:- National Cyber-security Plan, action plan and governance model -Review of the existing National Broadband Plan	No. of Documents	0	2
Component 3: - Proposal to update specific legislation to improve the telecommunications regulatory framework - Proposal to update specific legislation to improve the telecommunications regulatory framework	No. of Documents	0	2
Component 4: workshops	No. of Workshops	0	3
Outcome Indicators:			
Increased government awareness and understanding of the current status of broadband and cyber-security in the country and additional related action to accelerate the penetration, adoption and use of broadband services and development of cyber-security.	No. of citations of the TC products in national government strategic documents	0	3

Table 3.2: Budget of reference

Activities	Description	IDB	Total
Component 1: Diagnostic and Analysis of alternative infrastructure for broadband deployment and cyber-security	Consultancy: estimation of the required investment in infrastructure to achieve universality in broadband access and service; and estimation of the required investment in cyber-security infrastructure	230,000	230,000
Component 2: Development of a national Cyber-security Plan, action plan and governance model; including a proposal to update specific legislation to promote the telecommunications regulatory framework	Consultancy: identification of actions to promote cyber-security among institutions and development of the governance model that allows its effective execution. It also includes a review of the national broadband plan.	230,000	230,000
Component 3: Workshops to disseminate results and to provide light cyber-security training	Workshops conducted by consultants to present results and conduct light training after each of the Components 1, 2,	20,000	20,000
Contingences		20,000	20,000
Total		**500,000**	**500,000**

IV. EXECUTING AGENCY AND EXECUTING STRUCTURE

4.1 In response to the petition from the Ministry of Finance of Paraguay, the executing agency will be the IFT/CTI Division, which will operate in coordination with the staff of the Institution.

V. PROJECT RISKS

5.1 This project presents two risks that could affect the impact, quality or sustainability of the expected results: (i) lack of institutional capacity in Paraguay; and (ii) that the results of the project are not taken into account to increase broadband connectivity and cyber-security due to a lack of formal commitment to undertake regulatory and policy reform and deploy additional infrastructure once the project is finished.

5.2 The first risk will be mitigated by the fact that the project will be executed by the IFD/CTI Division, as per the government's request. In addition, the project will include a monitoring process throughout the implementation of the project to allow for the different Paraguayan institutions to get involved from the beginning to the end of the project.

5.3 The second risk is mitigated by the fact that this project is a direct response to the interest presented by the government to the Bank as it seeks to further promote broadband penetration and cyber-security in the country. Current efforts such as the ICTs plan (Plan Director de TICs) or the Computer Security Incident Response (CSIRTpy) team evidence the government's commitment to effectively address the broadband access and cyber-security gaps in the country, thus, there is

reason to believe that the government will find the resulting products of the project valuable for future undertakings.

VI. EXCEPTIONS TO THE POLICY OF THE BANK

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

VII. ENVIRONMENTAL STRATEGY

Given that the current TC revolves around a study, there are no social or environmental risks associated with it. This operation is classified as a Category “C” according to the classification toolkit of the Bank. (See link: IDBDocs#37789908).