

ADMINISTRATION AGREEMENT

between

THE INTER-AMERICAN DEVELOPMENT BANK

and

ISRAEL MINISTRY OF ECONOMY

regarding

**Project Specific Grant to the Inter-American Development Bank
for Project No. RG-T2788 titled,
“Improving Human Resources Capacity in Cybersecurity”**

THIS ADMINISTRATION AGREEMENT is entered into between the Inter-American Development Bank (the "Bank") and the Israel Ministry of Economy (the "Donor") (hereinafter together referred to as the "Parties").

WHEREAS, the Bank has approved Project No. RG-T2788 titled, "Improving Human Resources Capacity in Cybersecurity" (the "Project"), as described in the attached project document (the "Project Document");

WHEREAS, the Donor has agreed to support the execution of the Project by providing a project specific grant to be administered by the Bank; and

WHEREAS, the Bank is prepared to receive and administer the contribution funds to be made available by the Donor.

NOW, THEREFORE, the Parties hereby agree as follows:

1. The Donor will make available to the Bank a grant contribution in the amount of U.S.\$2,050,000.00 (two million fifty thousand dollars of the United States of America) (the "Contribution") to be administered by the Bank to co-finance the Project.
2. The Contribution will be solely for the purposes indicated in the Project Document. Any material deviations from the objectives and activities of the Project described in the Project Document will require the Donor's written approval.
3. Following the signature of this Administration Agreement by the Parties, the Donor will transfer the Contribution to the Bank in one single installment, upon the Bank's written request, to the account indicated by the Bank in writing (the "Account"). The Account is denominated in U.S. dollars and includes resources provided as grant funds by other donors for other Bank projects. The Contribution will be administered in the Account without distinction from other donors' contributions.
4. The Bank will administer the Contribution in accordance with the provisions of this Administration Agreement and the Bank's applicable policies and procedures. The Bank will exercise the same care in the discharge of its functions, as described in this Administration Agreement, as it exercises with respect to the administration and management of resources from other donors, and will have no further liability to the Donor in respect thereof.
5. The Contribution will be accounted for separately from the Bank's assets, and will be administered together with other contributions received by the Bank. The Bank may freely exchange the Contribution funds into other currencies as may facilitate their administration and disbursement. The Bank will not be responsible for foreign exchange risk in the receipt, conversion or administration of Contribution funds. Further, the Bank may at its discretion invest and reinvest the resources of the Contribution pending their disbursement in connection with the Project.



6. To assist in the defrayment of the administrative costs in relation to the Contribution, the Bank will charge and retain:
 - (a) a fee equal to five percent (5%) of the total amount of the Contribution at the time the Contribution is deposited by the Donor into the Account; and
 - (b) any investment income generated by the Contribution pending its disbursement towards the Project.
7. The Bank's procurement policies and procedures will be applicable to the procurement of goods and services, as well as the contracting of consulting services, carried out with the Contribution, as required by the different components of the Project. Further, the Donor accepts that:
 - (a) the resources of the Contribution will be completely untied; and
 - (b) the consultancy services financed with the Contribution may be provided and executed by companies, specialized institutions or individuals from any Bank member country.
8. The Donor will not be responsible for the activities of any person or third-party engaged by the Bank as a result of this Administration Agreement, nor will the Donor be liable for any costs incurred by the Bank in terminating the engagement of any such person.
9. Promptly following the completion of the Project, the Bank will submit to the Donor a final Project report. The Donor may also request a non-audited financial expense report of the Contribution. In addition, the Donor may request an "agreed upon procedures" report issued by an external auditor selected by the Bank on the use of the Contribution resources. The cost of such auditor's report will be borne by the Donor and will not be deducted from the Contribution. The Donor will reimburse the Bank for the cost of this report promptly after receiving a written request from the Bank. The Bank will not provide audited financial statements for the Account.
10. As soon as possible upon completion of the Project, the Bank will return to the Donor any remaining uncommitted Contribution funds, unless otherwise agreed to in writing by the Parties.
11. The Donor acknowledges that the Bank's commitment to use the Contribution as contemplated herein will be subject to the Bank's formalization of all internal approvals necessary for the Project and/or the Project Document.
12. The offices responsible for coordination of all matters and receiving any notice or request in writing in connection with this Administration Agreement or the Project are as follow:

(a) For the Bank:

- i. All communications pertaining to donor relations and resource mobilization will be directed to:

Inter-American Development Bank
1300 New York Avenue, NW
Washington, D.C. 20577
UNITED STATES OF AMERICA

Attention: Manager, Office of Outreach and Partnerships (ORP)
Tel.: +1 (202) 623-1583
Fax: +1 (202) 623-2543
E-mail: partnerships@iadb.org

- ii. Day-to-day communications regarding the management of the Contribution and the implementation of this Administration Agreement will be directed to:

Inter-American Development Bank
1300 New York Avenue, NW
Washington, D.C. 20577
UNITED STATES OF AMERICA

Attention: Chief, Grants and Co-financing Management Unit
Office of Outreach and Partnerships (ORP/GCM)
Tel.: +1 (202) 623-2018
Fax: +1 (202) 623-3489
E-mail: orp-gcm@iadb.org

(b) For the Donor:

Trade Mission
Embassy of Israel
3514 International Drive, NW
Washington, D.C. 20008
UNITED STATES OF AMERICA

Attention: Anat Katz, Head of Trade Mission
Tel.: +1 (202) 364-5695
Fax: +1 (202) 364-5647
E-mail: Anat.Katz@israeltrade.gov.il

13. This Administration Agreement will come into force on the date of its signature by each of the Parties.

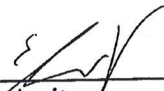
14. The Parties may amend any provision of this Administration Agreement in writing.



15. Subject to their respective policies and procedures with respect to the disclosure of information, the Parties may make this Administration Agreement publicly available.
16. Nothing in this Administration Agreement may be construed as creating an agency relationship between the Parties.
17. The Parties will seek to settle amicably any disputes that may arise from or relate to this Administration Agreement.

IN WITNESS WHEREOF, the Inter-American Development Bank and the Israel Ministry of Economy, each acting through its duly authorized representative, have signed this Administration Agreement in the English language as of the dates indicated below.


ISRAEL MINISTRY OF ECONOMY



Lang Amit
Director General

Date: 9/21/16


ISRAEL MINISTRY OF ECONOMY



Steinberg Yossi
Ministry Chief Accountant

Date: 9/21/16

**INTER-AMERICAN
DEVELOPMENT BANK**



Bernardo Guillamon
Manager, Office of Outreach and Partnerships

Date: 9/22/16

TC Document

I. Basic Information

▪ Country/Region:	Regional
▪ TC Name:	Improving human resources capacity in cybersecurity
▪ TC Number:	RG-T2788
▪ Team Leader/Members:	Miguel Porrúa (Team Leader, IFD/ICS); Antonio García Zaballos (IFD/CMF); Alejandro Pareja (IFD/ICS); Daniel Hincapié (ORP/PTR); Catalina García de Alba (IFD/ICS); Florencia Cabral (IFD/ICS); María Sofía Greco (LEG/SGO); y Claudia Ogliastro (ORP/GCM).
▪ Taxonomy:	Research and Dissemination
▪ Date of TC Abstract authorization:	N/A
▪ Beneficiary:	Latin America and the Caribbean Region
▪ Executing Agency:	The Bank through the Institutional Capacity of the State Division (IFD/ICS)
▪ Donors providing funding:	Government of Israel ¹
▪ IDB Funding Requested:	US\$2,050,000
▪ Local counterpart funding:	N/A
▪ Disbursement period:	42 months (execution period: 36 months)
▪ Required start date:	June 2016
▪ Types of consultants:	Individual consultants and consulting firms
▪ Prepared by Unit:	IFD/ICS
▪ Unit of Disbursement Responsibility:	Institutions for Development Sector (IFD/IFD)
▪ TC Included in Country Strategy:	N/A
▪ TC included in CPD:	N/A
▪ GCI-9 Sector Priority:	Institutions for growth and social welfare ²

II. Objectives and Justification of the TC

- 2.1 **Background and justification.** A report on cybersecurity in Latin America and the Caribbean (LAC) published in 2014³ indicates that just three countries in Latin America (Argentina, Brazil, and Colombia), generate 3.2% of the phishing attacks⁴ worldwide. The cyberspace where citizens manage many aspects of their lives is under growing threat. In 2014, more than 300 data breaches occurred, 348 million identities were exposed worldwide⁵ and almost half a million web attacks were blocked every day. At the same time, just 5 countries in LAC (Colombia, Jamaica, Panama, Trinidad and Tobago, and Uruguay) have set up cybersecurity strategies, and the majority of them do not have qualified human resources to face these threats that grow in number and sophistication.

¹ These funds will be administered by the IDB through a non-reimbursable Project-Specific Grant (PSG). The Government of Israel will contribute US\$2,050,000. This PSG will be administered by the IDB pursuant document SC-114. In accordance with that document, the commitment of the Government of Israel for the PSG will be established through a separate Administrative Agreement.

² 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 supports the strengthening of institutions, and has specifically recognized the need to improve policies and governmental action in the Information and Communication Technology sector (5.21 of the referenced Sector Strategy). Consistent with the Strategy, the Bank has approved a Broadband Special Program to accelerate the penetration rate and usage of broadband services in the Region (GN-2704). Citizen security is one of the main areas of the Strategy for institutions for growth and social welfare (IDB Document GN-2587). Finally, it was identified as a priority area that contributes to the objectives of the Bank's ninth capital increase, GCI-9 (Document of the Board of Directors AB-2764).

³ Latin American and Caribbean Cybersecurity Trends. OAS and Symantec. June 2014.

⁴ "The act of sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft". Webopedia.

⁵ Internet Cybersecurity Threat Report. Vol 20. Symantec. April 2015.

- 2.2 Israel is considered one of the most advanced countries worldwide in cybersecurity.⁶ It has more than 300 firms specialized in cybersecurity and most of the big cybersecurity companies have research and development centers in Israel⁷. The National Cyber Bureau of Israel operates under the umbrella of the Prime Minister and has the responsibility for the implementation of the cybersecurity strategy of Israel. In addition to Israel, countries generally recognized as cybersecurity leaders are the US, Sweden, Finland, Australia, South Korea and Estonia, among others.⁸ These countries can be a valuable source of experience for most of LAC countries that are taking initial steps to set up cybersecurity policies.
- 2.3 More than 50% of the Latin American and Caribbean population has access to the Internet, close to 350 million citizens.⁹ This important Internet population grows at a rate of 12% a year, the fastest in the world.¹⁰ In addition, the Latin American population is the biggest user of social networks worldwide in relative terms. Out of the top 10 countries using social media websites, 5 are from Latin America.¹¹ The region spends 8.1 hours per month on social media while the worldwide average is 5.2 hours.
- 2.4 Information and Communication Technologies (ICTs) have become the foundation of the efficient functioning of several key areas of LAC countries, from access to public services to the distribution of energy. Thanks to the Internet, Chileans can access 350 government procedures online and Ecuadoreans can fulfill their obligations through the Tax Office online.¹² ICTs are also present throughout the value generation chain in energy supply, water distribution, and transportation network or traffic control just to mention a few critical areas.
- 2.5 The advancement of Information and Communication Technologies in the region has transformed them into a relevant part of the economic activity of several countries. In 2013, ICTs contributed 4.5% of the GDP in Argentina, and 6% in Colombia. In the same year, Brazil invested in ICTs more than US\$50 billion. In Colombia, the ICT sector created more than 100,000 jobs during the period 2010-13.¹³ However, if the appropriate cybersecurity policies are not set up, this wealth is in danger of being wiped out by cybercrime. A recent report by the Center for Strategic International Studies estimates that cybercrime extracts between 15% and 20% of the value created by Internet, around US\$400 billion worldwide annually.¹⁴
- 2.6 In a study conducted by Trend Micro in 20 LAC countries, the cybersecurity authorities expressed that "threats are severe" and the majority of the interviewees mentioned that "the frequency of the attacks is growing or remains stable while those attacks are increasingly sophisticated." This same study shows that Government (51% of organizations that experienced attacks) and Energy (47%) are the most attacked sectors in the cyberspace. The study

⁶ <http://fortune.com/2015/09/01/why-israel-dominates-in-cyber-security/>

⁷ *Best Practices and Lessons Learned in the ICT Sector Innovation: a case study of Israel*. The World Bank. 2016. <http://pubdocs.worldbank.org/pubdocs/publicdoc/2016/1/868791452529898941/WDR16-BP-ICT-Sector-Innovation-Israel-Getz.pdf>

⁸ <http://thediplomat.com/2012/02/israel-china-and-cyber-security/>

⁹ <http://www.internetworldstats.com/stats2.htm>

¹⁰ <http://www.comscore.com/Insights/Events-and-Webinars/Webinar/2013/2013-Latin-America-Digital-Future-in-Focus>

¹¹ http://www.digitalstrategyconsulting.com/intelligence/2013/05/top_10_countries_for_social_media_engagement_time_spent.php

¹² <http://www.explored.com.ec/noticias-ecuador/el-sri-elimina-las-declaraciones-y-los-comprobantes-de-venta-fisicos-en-2013-570502.html>

¹³ OAS/Trend Micro - Cybersecurity and Critical Infrastructure Protection Report, Pages 21 and 22.

¹⁴ http://csis.org/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf

concludes that in order to protect LAC countries against cyber-attacks "budgets must be increased, capacity must be built and more information has to be shared".

- 2.7 The *Cybersecurity Report 2016: Are we ready in Latin America and the Caribbean?*, recently launched by the IDB and the Organization of American States (OAS), shows that 80% of the LAC countries don't have a cybersecurity strategy nor a plan to protect their national critical infrastructure.¹⁵ When asked about their perception on the degree of readiness to manage incidents in the cyberspace, just 2 countries out of 32¹⁶ responded that they were "prepared," "somewhat prepared" was the response of 13 of them and 5 others responded "unprepared." Eighty percent of the countries lack educational policies on cybersecurity, and in 85% of the countries prosecutors don't have the capacity of bring cybercrimes to trial. Another aspect of the lack of preparation of the region to face an insecure cyber environment is the fact that of the 26 IDB borrowing member-countries, just 12¹⁷ have set up Computer Emergency Response Teams (CERT) or Computer Security Incident Response Teams (CSIRT).¹⁸
- 2.8 Analyzed by subregion, the Report shows that a group of countries, such as Uruguay, Brazil, Mexico, Argentina, Chile, Colombia, and Trinidad and Tobago, are ahead of the rest and will need more advanced and specific support. The Caribbean region does better in the society, culture, and legal dimension, but is weak in the technological one. The Central American and Andean regions show a stronger position in the education and legal framework but a weak position in the policy and strategy as well as the technological one. The Southern Cone is better positioned in policy and strategy as well as society and culture but shows weaknesses in technology and education. In the education dimension no country reaches level 2 out of 5, and overall none reaches the middle point of the maturity model used in the Report.
- 2.9 The Regional Workshop on Cybersecurity Policies held at the IDB in October 2014 allowed the Bank to open a dialogue with the region's cybersecurity policy makers in order to know their needs and their commitment to work on solving them. The high level of attendance (80% of the LAC countries participated) and the level of responsibility of those attending show a clear commitment. A full day of discussions on their cybersecurity challenges was set up, and the participants transmitted to the IDB and the OAS a need for support in the following areas: (i) incident response capacities; (ii) lack of financial resources and of personnel training to implement a national CERT; (iii) lack of cybersecurity awareness and education; and (iv) improving countries' response capacity to cyber threats.¹⁹ Most panelists pointed out that countries should heavily invest in their organic capability, that is, skilled human resources and learn from the experience of the most advanced nations.
- 2.10 For the past two years, the Bank has contributed to LAC countries' efforts in cybersecurity by documenting the status of cybersecurity in the region through the 2016 Cybersecurity Report, as well as by organizing the Regional Workshop of Cybersecurity Policy makers,²⁰ both in collaboration with

¹⁵ *Cybersecurity Report 2016: Are we ready in Latin America and the Caribbean?*

¹⁶ The study targeted all OAS Latin American and Caribbean member countries (32).

¹⁷ <http://www.lacnic.net/en/web/lacnic/csirts>

¹⁸ CSIRT is a service organization that is responsible for receiving, reviewing, and responding to computer security incident reports and activity. CERT is a registered mark of Carnegie Mellon University that can be used just by authorized CSIRT.

¹⁹ Regional Workshop on Cyber Security Policies. Findings Report. Washington DC. October 22-24, 2014.

²⁰ <http://events.iadb.org/calendar/eventDetail.aspx?lang=en&id=4645&SP=Y>

the OAS. The knowledge and network developed will be of great value for the successful implementation of this technical cooperation.

- 2.11 **Objective.** The objective of this project is to assist beneficiary countries to strengthen the capacity of the institutions responsible for cybersecurity by providing government officials and policymakers access to training and lessons learned from the most advanced experiences worldwide.

III. Description of activities/components and budget

- 3.1 **Component 1: Knowledge generation and exchange.** The objective of this component is to facilitate the access to advanced cybersecurity experiences by appropriately documenting and disseminating them. The activities to be financed under this component are the following: (i) **Activity 1.1: Elaboration of a cybersecurity experience document:** preparation of a document including a compilation of the most remarkable cybersecurity solutions and experiences developed by Israel and other countries, as well as the most important lessons learned from these. The document will be produced in Spanish and English, and will take advantage of modern graphic design to increase its usability. This document will include the following aspects of each country analyzed: political and strategic framework, cultural and social aspects, educational matters, legal environment and ICT infrastructure. It will be a key tool to make LAC experts aware of the magnitude of the experience developed by Israel and its potential applicability to the region; (ii) **Activity 1.2: International workshops:** the workshops will convene policy makers and top managers in the area of cybersecurity and will include presentations and onsite visits. The agenda will focus on the key elements of a cybersecurity strategy and provide a comprehensive vision of cybersecurity. A total of two workshops are planned to be held in Israel as a leading country in the field of cybersecurity, but could be held in a different country if the dialogue with LAC countries indicate so, in which case it will have an Israeli presence; (iii) **Activity 1.3: LAC workshops:** with the aim of facilitating access to international experiences to as many LAC cybersecurity experts and managers as possible, a workshop with recognized international experts will be organized in a country in LAC to be defined. Throughout the life of this project, two workshops will be organized, and include Israeli experiences. It will focus in presenting practical cases and solutions related to the most important aspects of a cybersecurity strategy such as information sharing and analysis, monitoring tools, cybersecurity governance and coordination, cyber-attack prevention, critical infrastructure protection, CSIRTs for specific sectors among others; and (iv) **Activity 1.4. Elaboration of a database of cybersecurity best practices:** where key aspects of those international experiences are clearly identified and documented. Among these aspects: regulatory framework, cybersecurity governance, private sector participation, international coordination mechanism, citizen awareness and human resources capacity. The database will be hosted by the IDB and beneficiary countries will be able to access it online.
- 3.2 **Component 2. Tailor-made courses for cybersecurity managers.** To address the concerns previously mentioned about the need for qualified human resources in cybersecurity, several training activities will be conducted, focusing on the most important areas of a cybersecurity strategy. This training will be provided on site, in Israel, through the most important academic

institutions and experts in the country²¹. The National Cybersecurity Bureau (Office of the Prime Minister of Israel) will be responsible for the organization of these courses that will last between 10 and 15 days²². Two training shifts will be offered each year to train 35 participants annually. The content will be designed to address the specific qualification needs of each participant, taught by practitioners and designed for immediate applicability. Training will focus on areas such as: CERT organization and management, critical infrastructure protection, citizen awareness, international coordination and private sector participation among others.

- 3.3 **Component 3. Pilot projects design.** This component will provide consulting support for the design of pilot projects in the area of cybersecurity. These projects could focus in a specific area (legal framework, academic curriculum, ICT infrastructure, CERT, etc.) or be a comprehensive strategy to improve cybersecurity. Eleven pilot projects will be funded through this component.²³
- 3.4 In addition, travel expenses for Staff members of the Bank will be funded by this Project (unforeseen expenses). Such expenses are necessary and indispensable to reach the objective of the TC and will contribute to the attainment of Activities 1.2 and 1.3.
- 3.5 The expected result of this TC is to contribute to the strengthening of the human resources capacity in institutions responsible for cybersecurity throughout the LAC region, and provide them with knowledge to set up stable training plans that will keep their professionals abreast in the field of cybersecurity. Specific results are:

Indicative Results Matrix*

Definition	Unit of measure	Base Line	Target
Cybersecurity experiences and solutions documented in Spanish and English	Number of documents published	0	1
Cybersecurity managers and policy makers knowledgeable in the most advanced cybersecurity experiences	Number of cybersecurity managers and policy makers participating in the international workshops	0	28
Cybersecurity experts acquainted in the most advanced cybersecurity solutions worldwide	Number of cybersecurity experts participating in the LAC workshop	0	40
An online database documenting the cybersecurity strategies of 10 advanced countries in operation	Number of cybersecurity strategies documented	0	10
Government officials trained in cybersecurity matters	Number of government officials trained	0	80
Pilot projects designed and approved	Number of pilot projects approved	0	11

*See Detailed Results Matrix.

- 3.6 The total cost of this TC is US\$2,050,000 that will be contributed by the Government of Israel. Local contribution is not expected for this project.

²¹ Institutions such as Ben Gurion University Cyber Security Research Center, and The Blavatnik Interdisciplinary Cyber Research Center (ICRC) at Tel Aviv University, enjoy worldwide recognition in the field and could be potential providers of this formal training.

²² A call for candidates will be made to each country who will submit three candidacies. It is expected that one participant per country will be selected (the 9 countries at the lowest positions in the Cybersecurity Report 2016 will have two training spots per year instead of one). Eligibility criteria: (1) level of responsibility of the candidate (candidates with higher responsibility will be given priority); (2) at least a year of contractual relationship with the Government after the training is complete; (3) degree of connection to the course main topics. The costs associated with the participation of each participant to the course will be covered (i.e. airfare, local transportation, accommodation, meals and medical insurance).

²³ Eligibility criteria: (1) a country cannot receive support for more than one pilot; (2) pilot projects will support the design or implementation of cybersecurity strategies; (3) the topics of the pilot projects must support any of the 22 factors of maturity included in the Cybersecurity Report 2016 mentioned in footnote 14. Countries may submit projects at any time throughout the year, and those in compliance with the eligibility criteria will be selected on first-come-first-serve basis.

- 3.7 Resources of this project to be received from the Government of Israel will be provided to the Bank through a Project Specific Grant (PSG). A PSG is administered by the Bank according to the "Report on COFABS, Ad-Hocs and CLFGS and a Proposal to Unify Them as Project Specific Grants (PSGs)" (Document SC-114). As contemplated in these procedures, the commitment from the Government of Israel will be established through a separate administrative arrangement. Under such arrangement, the resources for this project will be administered by the Bank and the Bank will charge an administrative fee of 5% of the contribution, which is duly identified in the budget of this project. The 5% administrative fee will be charged after the contribution has been received.

Indicative Budget (US\$)*

Activity/Component	IDB Funding (PSG)	Local counterpart Funding	Total
Component 1	495,250	0	495,250
Component 2	621,250	0	621,250
Component 3	547,800	0	547,800
Project management and coordination	192,000	0	192,000
Monitoring and evaluation	45,000	0	45,000
Unforeseen expenses	46,200	0	46,200
Administrative fee (5%)	102,500	0	102,500
Total			2,050,000

*See Detailed Budget.

- 3.8 A midterm evaluation will be conducted to ascertain whether the project is advancing in accomplishing its objectives. This evaluation will be carried out based on personal interviews to the cyber security authorities who participated in the first Regional Exchange. This in-depth questionnaire will inquire, among other things, on the relevance of the topics treated, the usefulness of the knowledge documents produced as well as the quantity and quality of expertise exchanged. After the last activity, a final evaluation will be completed including both personal interviews and a focus group comprised of at least one cyber security authority per Bank region to assess the overall impact of the project.

V. Executing agency and execution structure

- 4.1 Over the past years, the Bank has undertaken several efforts to support cybersecurity in the region, thereby accumulating valuable experience in this area. In addition, it has particular technical and administrative expertise in the execution of Research and Dissemination projects; thus, it can ensure that administrative burdens can be reduced in the participating countries, particularly in the contracting of international experts, and that all LAC countries will benefit from the activities of this TC.
- 4.2 Given the complexity, workload and magnitude of this project, a project coordinator with cybersecurity expertise will be added to the IFD/ICS team (for two years, full-time) with the support of this technical cooperation. The project coordinator will be responsible for the management of the day-to-day activities of this project under the supervision of the e-government lead specialist of the Bank. The main activities to be undertaken by the project coordinator are: activities for planning and implementation, contract supervision, project communications and periodic reporting. Prior to the execution of the project activities in any of the beneficiary countries, the Bank shall obtain the corresponding non-objection from the respective country authority.

- 4.3 A selection Committee with one representative from the IDB, one from the Government of Israel and academic institution will be setup and will be responsible for the definition of the list of participants, and the pilot projects, eligible under Component 2 and Component 3, respectively. Prior to the selection and hiring of the consultants or consulting firms that will be responsible for the provision of the training services for the execution of Component 2, the Bank will consult and seek collaboration from the National Cyber Bureau.
- 4.4 The Bank will contract individual consultants, consulting firms and non-consulting services in accordance with Bank's current procurement policies and procedures.
- 4.5 The project team will be responsible for the preparation and submission to the donor of the project reporting in compliance with the stipulation of the Administration Agreement. If at the end of project execution the project was closed with a positive uncommitted and unspent balance, the project team will be responsible for informing ORP/GCM to transfer the unspent balance as agreed to by the donor and the Bank pursuant to the terms of the PSG Administration Agreement.

VI. Major issues

- 5.1 The identification of individual country needs will be undertaken by means of a survey, whose results will support the design of the training activities and the planning of the consulting support provided through Component 3. Since governments frequently complain about the numerous questionnaires they have to complete every year there is a risk of not getting enough responses to elaborate a well-informed needs assessment. The risk will be mitigated by indicating in the form that in order to benefit from the training support provided by this project, the country has to submit the questionnaire.
- 5.2 In some countries, institutional weakness and fragmentation poses a challenge for the stability of cybersecurity initiatives, including the retention of human resources. This risk will be mitigated by promoting the set-up of CERTs, as well as by placing an emphasis on providing advice on defining the appropriate institutional architecture to manage a stable cybersecurity program.
- 5.3 Given the limited availability of human resources in the institutions responsible for cybersecurity in LAC, government might be reluctant to let their cybersecurity experts to be away from office for a certain period of time even if for training purposes. This risk will be mitigated by limiting the length of the training activities and by assuring the availability of daily time to maintain contact their offices of origin.

VII. Exceptions to Bank policy

- 6.1 No exceptions to Bank policy are foreseen.

VIII. Environmental and Social Strategy

- 7.1 According to the Environment and Safeguards Compliance Policy (OP-703), the TC has been classified as category C. No potential negative environmental and/or social impacts of the TC were identified and therefore no mitigation strategy is required to address any impact.

Required Annexes:

- Terms of Reference
- Procurement Plan

TERMS OF REFERENCE
(Consulting Firm)

IFD/ICS

RG-T2788: Improving Human Resources Capacity in Cybersecurity

Component 2: Training

I. BACKGROUND

- 1.1 A report on cybersecurity in Latin America and the Caribbean (LAC) published in 2014¹ indicates that just three countries in Latin America, Brazil, Colombia and Argentina, generate 3.2% of the phishing attacks² worldwide. The cyberspace where citizens manage many aspects of their lives is under growing threat. In 2014, more than 300 data breaches occurred, 348 million identities were exposed³ and almost half a million web attacks were blocked every day. At the same time, just 5 countries in LAC have set up cybersecurity strategies and the majority of them do not have the qualified human resources to face these threats that grow in number and sophistication.
- 1.2 Israel is considered one of the most advanced countries worldwide in cybersecurity⁴. It has a more than 300 firms specialized in cybersecurity and most of the big cybersecurity companies have research and development centers in Israel⁵. The National Cyber Bureau operates under the umbrella of the Prime Minister and has the responsibility for the implementation of the cybersecurity strategy of Israel. In addition to Israel, countries generally recognized as cybersecurity leaders are the US, Sweden, Finland, Australia, South Korea and Estonia among others⁶. These countries can be a valuable source of experience for most of LAC countries that are taking initial steps to set up cybersecurity policies.
- 1.3 More than 50% of the Latin American and Caribbean population have access to the internet, close to 350 million citizens⁷. This important internet population grows at a rate of 12% a year, the fastest in the world⁸. In addition, Latin American population is the

¹ Latin American and Caribbean Cybersecurity Trends. OAS and Symantec. June 2014

² "The act of sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft". Webopedia.

³ Internet Cybersecurity Threat Report. Vol 20. Symantec. April 2015

⁴ <http://fortune.com/2015/09/01/why-israel-dominates-in-cyber-security/>

⁵ *Best Practices and Lessons Learned in the ICT Sector Innovation: a case study of Israel*. The World Bank. 2016. <http://pubdocs.worldbank.org/pubdocs/publicdoc/2016/1/868791452529898941/WDRI6-BP-ICT-Sector-Innovation-Israel-Getz.pdf>

⁶ <http://thediplomat.com/2012/02/israel-china-and-cyber-security/>

⁷ <http://www.internetworldstats.com/stats2.htm>

⁸ <http://www.comscore.com/Insights/Events-and-Webinars/Webinar/2013/2013-Latin-America-Digital-Future-in-Focus>

biggest user of social networks worldwide in relative terms. Out of the top 10 countries using social media websites, 5 are from Latin America⁹. The region spends 8.1 hours per month on social media while the worldwide average is 5.2 hours.

- 1.4 Information and Communication Technologies have become the foundation of the efficient functioning of several key areas of Latin American and Caribbean countries, from access to public services to the distribution of Energy. Thanks to the internet, Chileans can access 350 government procedures online and Ecuadoreans fulfill their obligations with the Tax office online¹⁰. ICTs are also present throughout the value generation chain in energy supply, water distribution, and transportation network or traffic control just to mention a few critical areas.
- 1.5 The advancement of Information and Communication Technologies in the region has transformed them into a relevant part of the economic activity of several countries. In Argentina, ICTs amount to 4.5 % of the GDP while in Colombia reaches 6%. Brazil itself has invested in ICTs more than US\$50 billion in 2013 and in Colombia the ICT sector has created more than 100,000 jobs¹¹. However, if the appropriate cybersecurity policies are not set up this wealth is in danger of being wiped out by cybercrime. A recent report by the Center for Strategic International Studies estimates that cybercrime extracts between 15% and 20% of the value created by Internet, around US\$ 400 billion worldwide annually¹².
- 1.6 In a study conducted by Trend Micro in 20 Latin America and the Caribbean countries, the cybersecurity authorities expressed that “threats are severe” and the majority of the interviewees mentioned that “the frequency of the attacks is growing or remains stable while those attacks are increasingly sophisticated”. This same study shows that Government (51% of organizations that experienced attacks) and Energy (47%) are the most attacked sectors in the cyberspace. The study concludes that in order to protect LAC countries against cyber-attacks “budgets must be increased, capacity must be built and more information has to be shared”
- 1.7 A recent report launched by the IDB and the OAS shows that 80% of the Latin American and Caribbean countries don’t have a cybersecurity strategy nor a plan to protect their national critical infrastructure¹³, When asked about their perception on the degree of

⁹ http://www.digitalstrategyconsulting.com/intelligence/2013/05/top_10_countries_for_social_media_engagement_time_spent.php

¹⁰ <http://www.explored.com.ec/noticias-ecuador/el-sri-elimina-las-declaraciones-y-los-comprobantes-de-venta-fisicos-en-2013-570502.html>

¹¹ https://www.sites.oas.org/cyber/Certs_Web/OEA-Trend%20Micro%20Reporte%20Seguridad%20Cibernetica%20y%20Proteccion%20de%20la%20Inf%20Critica.pdf Pag. 21 and 22.

¹² http://csis.org/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf

¹³ [Cybersecurity Report 2016: Are we ready in Latin America and the Caribbean?](#)

readiness to manage incidents in the cyberspace just 2 countries out of 32¹⁴ responded that they were “prepared”. “Somewhat prepared” was the response of 13 of them and “Unprepared” was responded by 5. 80 % of the countries lack educational policies on cybersecurity and in 85% of the countries prosecutors don’t have the capacity of bring cybercrimes to trial. Another aspect of the lack of the preparation of the region to face an insecure cyber environment is the fact that of the 26 IDB country clients, just 12¹⁵ have set up CERTs (Computer Emergency Response Team) or CSIRTs (Computer Security Incident Response Team)¹⁶.

- 1.8 In addition, during the Regional Workshop on Cybersecurity Policies held at the IDB in October 2014 and attended by cybersecurity authorities from 27 LAC countries the following aspects were mentioned as main concerns: (i) incident response capacities; (ii) lack of financial resources and of personnel training to implement a national CERT; (iii) lack of cybersecurity awareness and education; and (iv) improving countries’ response capacity to cyber threats¹⁷. Most panelists pointed out that countries should heavily invest in their organic capability, that is, skilled human resources and learn from the experience of the most advanced nations.
- 1.9 **Objective.** The objective of the project is to assist beneficiary countries to strengthen the institutional capacity of the institutions responsible for cybersecurity by providing access to training and lessons learned from the most advanced cybersecurity experiences worldwide.
- 1.10 For the past two years the Bank has contributed to LAC countries’ efforts in cybersecurity by documenting the status of cybersecurity in the region through the *2016 Cybersecurity Report: Are we ready in Latin America and the Caribbean?* As well as by organizing the Regional Workshop of Cybersecurity Policy makers¹⁸, both in collaboration with the OAS. The knowledge and network developed will be of great value for the successful implementation of this technical cooperation.

II. CONSULTANCY OBJECTIVES

- 2.1 The objective of this consultancy is to undertake the tasks associated with Component 2 of this project which focuses on providing customized training on cybersecurity to 70 government officials from Latin American and Caribbean countries. The contracted firm

¹⁴ The study targeted all OAS Latin American and Caribbean countries (32).

¹⁵ <http://www.lacnic.net/en/web/lacnic/csirts>

¹⁶ CSIRT, a CSIRT is a service organization that is responsible for receiving, reviewing, and responding to computer security incident reports and activity. CERT, is a registered mark of Carnegie Mellon University that can be used just by authorized CSIRTs.

¹⁷ Regional Workshop on Cyber Security Policies. Findings Report. Washington DC. October 22-24, 2014.

¹⁸ <http://events.iadb.org/calendar/eventDetail.aspx?lang=en&id=4645&SP=Y>

in coordination with the Government of Israel will undertake all necessary activities to assure the provision of training on the topics indicated as a priority by the selected participants.

- 2.2 Four training activities will be organized. In between 15 and 20 participants will be trained in each of the activities for a total of 70 participants during 2 years.

III. ACTIVITIES AND PRODUCTS

The contractor will undertake the following activities:

1. Collaborate in the participants' selection process and elaborate an individual profile of each participant that includes his training needs.
2. Provide travel services to the participants from their countries of origin to the city in Israel where the training will take place.
3. Provide full accommodation in Israel to the participants as well as local transportation when necessary to receive the planned training.
4. To support the Government of Israel in organizing all training activities.
5. To manage and provide all the logistic support required to undertake the training activities.
6. To hire, when necessary as per the request of the Government of Israel, experts to provide the planned training.
7. To conduct an evaluation at the end of each training activity through an evaluation form to be elaborated in coordination with the IDB and the Government of Israel.
8. To elaborate a report after each training activity including the training received by each participant as well as a discussion on his performance (this information will be provided by the professors and the Government of Israel).

Products. As a result of this consultancy, the following products will be delivered:

1. An online digital database of all participants in the training activities (at the end of the contract this database will be transferred to the IDB) including their profiles and the training received.
2. A final report on all training provided through the duration of the contract. It will include: participants profiles, experts profiles, topics taught to each participant
3. A final evaluation report on the level of satisfaction of the participants, the degree of applicability of the acquired knowledge to their daily activities and the suggestions to improve future training activities.

IV. CHARACTERISTICS OF THIS CONSULTANCY

Type of Consultancy: Consulting Firm

Starting date and duration: Upon contract signing, 2 years

Working place/travels: This consultancy will be carried out by a consulting firm. Although the tasks may be carried out in the country of origin, the firm might be required to travel to LAC countries.

Qualifications: The firm will have extensive experience in organizing training activities for senior government officers and policy makers. This experience includes both the academic and logistics aspect of organizing training activities. The firm will have experience working with Latin American and Caribbean countries.

V. METHOD OF PAYMENT

Payment will be made as per the following schedule, upon approval by the Team Leader responsible for this project (see item VI below):

Schedule of payments:

- (i) 25% upon contract signature;
- (ii) 20% upon successfully organizing half of the planned training activities;
- (iii) 25% upon approval of draft report on all training provided;
- (iv) 30% upon approval of final evaluation report.

VI. COORDINATION

The supervision and coordination of this consultancy will be the responsibility of Mr. Miguel Porrúa, Modernization of the State Lead Specialist, (IFD/ICS), Team Leader of this operation, mporrúa@iadb.org tel. (202) 312-4102.

PROCUREMENT PLAN

No. Ref.	Description and type of the procurement contract	Estimated contract cost US\$	Procurement method	Review (ex-ante or ex-post)	Source of financing and percentage			Prequalification (Yes/No)	Estimated dates		Status (pending, in progress, awarded, cancelled)	Comments
					IDB %	Local / other %			Publication of specific procurement notice	Completion of contract		
1	GOODS											
	Component 1. Activity 1.4 Online database/website	10,000	PC	ex-post	100%	0%		No	N/A		Pending	
2	WORKS											
	N/A											
3	NON-CONSULTING SERVICES											
	Component 1. Activity 1.2 International Workshop 1 Plane tickets, per diem,	120,625	PC	ex-post	100%	0%		No	N/A		Pending	
	Component 1. Activity 1.2 International Workshop 2 Plane tickets, per diem	120,625	PC	ex-post	100%	0%		No	N/A		Pending	
	Component 1. Activity 1.3 International Workshop 1 Plane tickets and per diem	94,000	PC	ex-post	100%	0%		No	N/A		Pending	
	Component 1. Activity 1.3 International Workshop 2 Plane tickets, per diem	94,000	PC	ex-post	100%	0%		No	N/A		Pending	
4	CONSULTING SERVICES (Individual)											
	Component 1. Activity 1.1 Document elaboration	25,000	IICC	ex-post	100%	0%		No	N/A		Pending	
	Component 1. Activity 1.1 Graphic Design	6,000	IICC	ex-post	100%	0%		No	N/A		Pending	
	Component 1. Activity 1.4 Best practices documentation	25,000	IICC	ex-post	100%	0%		No	N/A		Pending	
	Component 3. Consultant 1	36,000	IICC	ex-post	100%	0%		No	N/A		Pending	
	Component 3. Consultant 2	36,000	IICC	ex-post	100%	0%		No	N/A		Pending	

No. Ref.	Description and type of the procurement contract	Estimate of contract Cost US\$	Procure ment method ¹	Review (ex- ante or ex- post)	Source of financing and percentage			Prequal- ification (Yes/No)	Estimated dates		Status, in progress, awarded, cancelled)	Comments
					IDB %	Local/ other %			Publication of specific procurement notice	Completion of contract		
	Component 3. Consultant 3	36,000	IICC	ex-post	100%	0%		No	N/A			
	Component 3. Consultant 4	36,000	IICC	ex-post	100%	0%		No	N/A		Pending	
	Component 3. Consultant 5	36,000	IICC	ex-post	100%	0%		No	N/A		Pending	
	Component 3. Consultant 6	36,000	IICC	ex-post	100%	0%		No	N/A		Pending	
	Component 3. Consultant 7	36,000	IICC	ex-post	100%	0%		No	N/A		Pending	
	Component 3. Consultant 8	36,000	IICC	ex-post	100%	0%		No	N/A		Pending	
	Component 3. Consultant 9	36,000	IICC	ex-post	100%	0%		No	N/A		Pending	
	Component 3. Consultant 10	36,000	IICC	ex-post	100%	0%		No	N/A		Pending	
	Component 3. Consultant 11	36,000	IICC	ex-post	100%	0%		No	N/A		Pending	
	Project Management and Coordination	192,000	IICC	ex-post	100%	0%		No	N/A			
	Monitoring and evaluation	45,000	IICC	ex-post	100%	0%		No	N/A		Pending	
5 CONSULTING SERVICES (Firms)												
	Component 2: Training in Israel	621,250	QCBS	ex-post	100%	0%		No	N/A		Pending	

¹ Goods and Works: ICB: International competitive bidding; LIB: limited international bidding; NCB: national competitive bidding; PC: price comparison; DC: direct contracting; FA: force account; PSA: Procurement through Specialized Agencies; PA: Procurement Agents; IA: Inspection Agents; PLFI: Procurement in Loans to Financial Intermediaries; BOO/BOT/BOOT: Build, Own, Operate/Build, Operate, Transfer/Build, Own, Operate, Transfer; PBP: Performance-Based Procurement; PLGB: Procurement under Loans Guaranteed by the Bank; PCP: Community participation procurement; Consulting Firms: QCBS: Quality- and Cost-Based Selection QBS: Quality-Based Selection FBS: Selection under a Fixed Budget; LCS: Least-Cost Selection; CQS: Selection based on the Consultants' Qualifications; SSS: Single-Source Selection. Individual Consultants: NICQ: National Individual Consultant selection based on Qualifications; IICC: International Individual Consultant selection based on Qualifications.