ANNEX A

HRD Terms of Reference

Cybersecurity Knowledge Generation Consultant

Regional

The IDB Group is a community of diverse, versatile, and passionate people who come together on a journey to improve lives in Latin America and the Caribbean. Our people find purpose and do what they love in an inclusive, collaborative, agile, and rewarding environment.

About this position

We are looking for a Knowledge Generation Consultant for the generation of knowledge materials for cybersecurity.

You will work in The Innovation in Citizen Services (ICS) division part of Institutions for Development (IFD) department. ICS mission is to strengthen the institutional capacity of the state to deliver better services to citizens using digital solutions and innovation, to support to the modernization of public management, and to promote citizen safety and security. Because of its wide range of activities, ICS is organized in three clusters.

The Data-Driven Digital Government Cluster (DDG) supports countries of the Region in improving the quality of services for their citizens and businesses. To do so, DDG promotes the operational efficiency in government agencies at all levels, through digital transformation and the use of information technologies. The Public-Sector Management Cluster (PSM) supports the strengthening of core government functions, to enhance their capacity to implement policies. The Citizen Security and Justice Cluster (CSJ) promotes investments in social prevention, security management and access to justice services. Digital Government and Cybersecurity activities are managed by the DDG cluster.

With the technical and financial support of the governments of Israel, South Korea and Spain, the IDB is undertaking a comprehensive plan to support LAC governments in designing and implementing digital government and cybersecurity initiatives. You will be a key part of this plan.

What you'll do:

- Support the design, generation and dissemination of knowledge products of best practices, policies, technologies and methodologies by organizing data, coordinating with other team members, following-up on the design and refinement of the materials produced, helping design and produce additional related materials, supporting launch processes and campaigns, and related promotional activities.
- Review methodological and sectorial documents and coordiante their preparation for publication.
- Prepare and design presentations, create document templates, reports and supporting material for meetings and events.
- Elaborate microcourse contents including editing videos and generating a final LMS package for publication.

Deliverables and Payments Timeline:

Payment will be made against delivery and approval of four knowledge products.

Deliverable #	Percentage	Product	Planned Date to Submit
1	16.6%	Video editing and finalizing an LMS (content files) package for micro course publication	April 2023
2	16.6%	Executive presentations and reports design	July 2023
3	16.6%	Methodological documents and publications review and publication coordination, group 3	August 2023
4	16.6%	Methodological documents and publications review and publication coordination, group 4	October 2023
5	16.6%	Sectoral cybersecurity publications, documents and drafts review, group 1	December 2023
6	16.6%	Sectoral cybersecurity publications, documents and drafts review, group 2	February 2024

What you'll need

- **Education:** Bachelor's degree in an Engineering-related discipline
- **Experience:** At least Two years of relevant professional experience, or the equivalent combination of education and experience. Experience in planning, designing and developing learning materials required.
  Core and Technical Competencies:
  Expertise in MS Microsoft Office suite and design software required. Excellent ability to work independently and as part of a team, and to communicate effectively both orally and in writing. Efficient and accurate with details. Strong organizational skills.
- **Languages:** Proficiency in Spanish and English, spoken and written, is required. Additional knowledge of French and Portuguese is preferable.

Key skills:

HRD Terms of Reference

- Learn continuously
- Collaborate and share knowledge
- Focus on clients
- Communicate and influence
- Innovate and try new things

Requirements:

- **Citizenship:** You are a citizen of one of our 48-member countries.
- **Consanguinity**: You have no family members (up to the fourth degree of consanguinity and second degree of affinity, including spouse) working at the IDB, IDB Invest, or IDB Lab.
- **COVID-19 considerations:** the health and safety of our employees are our number one priority. As a condition of employment, IDB/IDB Invest requires all new hires to be fully vaccinated against COVID-19.

Type of contract and duration:

- **Type of contract:** Products and External Services Consultant (PEC)
- **Length of contract:** 210 days in a period of 10 months

What we offer

The IDB group provides benefits that respond to the different needs and moments of an employee's life. These benefits include:

- A competitive compensation package.
- A flexible way of working. You will be evaluated by deliverable.

Our culture

At the IDB Group we work so everyone brings their best and authentic selves to work, willing to try new approaches without fear, and where they are accountable and rewarded for their actions.

Diversity, Equity, Inclusion and Belonging (DEIB) are at the center of our organization. We celebrate all dimensions of diversity and encourage women, LGBTQ+ people, persons with disabilities, Afro-descendants, and Indigenous people to apply.

We will ensure that individuals with disabilities are provided reasonable accommodation to participate in the job interview process. If you are a qualified candidate with a disability, please e-mail us at diversity@iadb.org to request reasonable accommodation to complete this application.

Our Human Resources Team reviews carefully every application.

About the IDB Group

ANNEX A

HRD Terms of Reference

The IDB Group, composed of the Inter-American Development Bank (IDB), IDB Invest, and the IDB Lab offers flexible financing solutions to its member countries to finance economic and social development through lending and grants to public and private entities in Latin America and the Caribbean.

About IDB

We work to improve lives in Latin America and the Caribbean. Through financial and technical support for countries working to reduce poverty and inequality, we help improve health and education and advance infrastructure. Our aim is to achieve development in a sustainable, climate-friendly way. With a history dating back to 1959, today we are the leading source of development financing for Latin America and the Caribbean. We provide loans, grants, and technical assistance; and we conduct extensive research. We maintain a strong commitment to achieving measurable results and the highest standards of integrity, transparency, and accountability.

Follow us:

https://www.linkedin.com/company/inter-american-development-bank/

https://www.facebook.com/IADB.org

https://twitter.com/the_IDB

HRD Terms of Reference

ANNEX A

Contract #: C- Click here to enter text

TC #: RG-T4135

Terms of Reference Lump Sum Contract

Logistical support for IDB delegation to Cybertech 2024 & Cyberweek 2023 Conferences

Strengthening Cybersecurity Capacity in LAC

1. Background and Justification

1.1. Information and Communication Technologies (ICTs) have become the foundation of the efficient functioning of many key areas in Latin American and the Caribbean (LAC) countries, from access to public services to the generation and supply of healthcare, energy, water distribution, and transportation infrastructure, just to mention a few critical areas. The cyberspace, the online world of computer networks and the Internet, became the medium in which people, companies, governments, and machines communicate with each other and carry out transactions. This new ecosystem has also seen the emergence of novel specific harms such as financial theft, service disruption, information theft, cyber terrorist attacks, and cyber espionage. These threats have only grown over recent years. The 2018 report by McAfee and the Center for Strategic and International Studies (CSIS) on the economic impact of cybercrime, estimated that this activity costed the world economy around $600 billion annually, or 0.8% of the global GDP, up from the estimated 0.7% in 2014. The most recent December 2020 release of the same report concluded that cybercrime now costs more than US$1 trillion, or over 1% of the global GDP.[1] Ransomware as a threat has evolved as well; such attacks are increasingly targeted, require higher ransom demands, and apply ever more sophisticated mechanisms. Many cyber threats rely on searching the Internet for vulnerable devices and networks, which leaves the increasing number of online users in developing countries with weak online security measures constantly exposed to potential attacks. In particular, the challenges posed by the COVID-19 pandemic, and the widespread move to remote work, set the stage for a spike in some forms of cyber threats, such as phishing and malware campaigns. Moreover, the Check Point Research 2021 Security Report[2] showed that over the first few months of 2020, almost a million attack attempts against Remote Desktop Protocol (RDP) connections, widely used among organizations for employees' remote connections, were observed every day. In fact, RDP attacks were the most popular form of cyberattack, surpassing even phishing emails. According to the ESET Latin America 2021 Security Report, in the LAC region, the number of RDP brute force attacks increased by 704% in 2020.[3] These trends only reaffirm our certainty that

1 The Hidden Cost of Cybercrime, McAfee & CSIS.
2 Check Point Research 2021 Security Report.
3 ESET Latin America 2021 Security Report.
4 Argentina, Brazil, Dominican Republic, Jamaica, Panama, Paraguay, and Uruguay.

the sophistication of attacks and economic motivation driving cybercrime will only continue to intensify.

1.2. In this context, being prepared, and knowing where we stand, is key. The Inter-American Development Bank (IDB) carries out assessments to capture the evolving capacities of its member states to defend against the growing threats in the cyberspace. The 2020 Regional Cybersecurity Maturity Report: “Risks, Progress and the Way Forward in Latin America and the Caribbean”, developed in partnership with the Organization of American States (OAS), showed that countries were in varying stages of development in their preparedness to face cybersecurity challenges, but generally still had ample room for improvement. While in 2016, the year of the report’s first edition, 80% of the countries in the region did not have a national cybersecurity strategy in place, this number was only down to 60% in 2020. Furthermore, only a few countries manage the exposure of their critical infrastructure –such as their energy, healthcare, telecommunications, transportation, water supply, and financial sectors– to cyberattacks. As revealed by the 2020 Report, only 7 countries of the 32 assessed had a critical infrastructure protection plan in place.[4] This is one of the most worrying findings of all, considering the catastrophic impact that attacks on these sectors could have not only on national economies, but on the lives of all their citizens.

1.3. In terms of countries’ capacity to manage and respond to cybersecurity incidents, the same study found that 63% of countries had security incident response teams in place, such as Computer Emergency Response Teams (CERTs) or Computer Security Incident Response Team (CSIRTs). However, of the 20 countries that did, only 3 had reached advanced maturity in their ability to coordinate such responses. In fact, 23 out of the 32 countries were still in an initial stage of maturity in this respect. This finding called attention to the general need for countries to strengthen the capacity of their teams to effectively coordinate their responses to cyber incidents.

1.4. In light of this worldwide movement to raise awareness on the importance of proactive Cyber Defense and in accordance with the IDB's commitment to safeguarding the interests of Latin America and the Caribbean Region (LAC), and with support from the Government of Israel, the IDB approved in 2021 the technical cooperation “Strengthening Cybersecurity Capacity in Latin America and the Caribbean” (RG-T4010), whose aim 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.

1.5. As a result of these efforts, the Bank has seen a significant increase in demand by IDB member countries for technical and operational support in cybersecurity. This demand is expected to continue growing in the coming years, because of countries’ increased awareness of the importance of protecting their cyberspace, on the national, sectoral, and organization-specific levels. For example, a great deal of public attention was drawn to the publication of "Israeli Cybersecurity Methodologies", a series of publications with 12 volumes to date, which have been translated into Spanish based on knowledge generated by the Israeli National Cybersecurity Directorate (INCD). These documents have had over 1000 downloads in less than a month of their release.

1.6. Israel continues to be one of the most advanced countries worldwide in cybersecurity.[5] It has more than 500 firms specialized in cybersecurity and most of the big cybersecurity companies have research and development centers in Israel.[6] The National Cyber Directorate of Israel operates within the Prime Minister's Office and has the responsibility for implementing Israel's cybersecurity strategy.

2. Objectives

2.1. The objective of this contract is to provide the necessary on-site logistical support for two delegations of public officials from Latin America and the Caribbean, and IDB personnel. The first will be the CyberWeek 2023 Conference in Tel Aviv, Israel between June 23rd and June 30th but may be rescheduled or not be realized, according to circumstances. The second, will take part during the first semester of 2024's Cybertech Conference in Tel Aviv, Israel. The consulting firm shall accompany the delegations, directly provide transportation to and from the site of the conferences and Tel Aviv airport, contract lodging for the groups, coordinate some of the meals, and generally support the execution of the visit's agendas, in close consultation with the IDB project team (the "IDB Team"), integrated by Ariel Nowersztern (arieln@iadb.org) and Santiago Paz Gonzalez (santiagopaz@iadb.org).

3. Key Activities

3.1. Manage the logistic aspects of the delegations as agreed in detailed plans, which may include among others: accompany the delegations and provide other tourism services and assistance as necessary; contract and directly pay the lodging for the IDB delegations in Tel Aviv; carry out airport transfers upon arrival and departure; provide transportation with guide to and from all site visits as per the agenda of activities; coordinate and pay for meals provided in the context of the visit's agenda; provide prepaid cards to cover participant expenses not directly provided for; hand in print packages with welcome information; order and deliver souvenirs.

3.2. Note: Both delegations may be rescheduled, reprogrammed in agreement with the consulting firm, or cancelled.

Payment Schedule

Payment will be made following the cost-per-unit specified in the firm's price proposal, which may be updated according to market prices at the time of booking, for the real number of units provided or anticipated at the time of invoice submission. The consulting firm shall include the detailed cost calculations in invoices for IDB approval. Disbursements will be executed as per the following schedule:

Delegation # 1: Cyberweek 2023

Percentage	Expected
60%: of the delegation's itemized planned budget at the time, as approved by the IDB	Within 2 weeks before activity start date

5 https://www.statista.com/statistics/1003442/israel-cyber-security-companies/#:~:text=This%20statistic%20shows%20the%20number,of%20450%20companies%20in%202018.

6 Advanced Experiences in Cybersecurity Policies and Practices: An Overview of Estonia, Israel, South Korea, and the United States. Inter-American Development Bank. 2016.

40%: completing to 100% of actual costs incurred for services rendered, as approved by the IDB	Within 2 weeks after activity end date

Delegation # 2: Cybertech 2024 or another similar delegation

Percentage	Expected
30%: of the delegation's planned itemized budget at the time, as approved by the IDB	Within 1 week of contract signature
30%: completing to 60% of the delegation's itemized budget at the time, as approved by the IDB	Within 2 weeks before activity start date
40%: completing to 100% of actual costs incurred for services rendered, as approved by the IDB	Within 2 weeks after activity end date

4. Acceptance Criteria

   The consulting firm shall maintain regular communication with the IDB Team in carrying out the activities described in this contract. All services to be contracted by the consulting firm must be presented to and approved by the IDB Team before any agreements with service providers are finalized. The consulting firm shall obtain the IDB Team's approval of each deliverable before associated payments will be processed.

5. Supervision

   The IDB Team will supervise execution of the activities and completion of the deliverables indicated in these terms of reference and approve all associated payments.

ANNEX A