PCC.I/RES. 166 (XVI-10) [1]

ITU AND CITEL REGIONAL CYBERSECURITY CAPACITY BUILDING WORKSHOP FOR THE AMERICAS "INTERNATIONAL COOPERATION FOR BUILDING A CULTURE OF HEMISPHERIC CYBERSECURITY"

The XVI Meeting of Permanent Consultative Committee I: Telecommunications/ Information and Communication Technologies (PCC.I),

CONSIDERING:

a) That PCC.I has recognized the central role of telecommunications in cybersecurity, and has created its own work program to focus and coordinate technical standardization and highlight regulatory issues associated with developing a culture of cybersecurity in the Region;

b) That ensuring the security of information systems is a priority matter for the hemisphere, as information networks play an important part in the critical infrastructure of countries, their economies, and societies;

c) That CITEL has fostered dialog in the past with the International Telecommunication Union (ITU) on Network and Cyber security, taking into account the Standardization work of Study Group 17 and the ongoing activity in the ITU-D sector (Question 22/1);

d) That CITEL is working, with the Inter-American Committee against Terrorism (CICTE) and the Justice Ministers and Attorneys General of the Americas (REMJA) of the Organization of American States (OAS), in a coordinated manner to advance the objectives of the hemisphere related to these important matters,

RECOGNIZING:

a) That CITEL supports an active multi-disciplinary approach to cybersecurity that pools its efforts with the efforts and expertise of CICTE and REMJA;

b) That the Comprehensive Inter-American Strategy to combat threats to cybersecurity relies on the efforts and specialized knowledge of CITEL, CICTE, and REMJA;

c) That a joint CITEL/ITU workshop will advance greater understanding of the critical issues related to cybersecurity for state and national governments and will provide a forum for information sharing, human capacity development, and continued collaboration among participants,

RESOLVES:

1. That PCC.I hold a one-day joint ITU and CITEL Regional Cybersecurity Capacity Building Workshop for the Americas on November 1, 2010 the day before of the XVII Meeting of CITEL PCC.I, based on the draft agenda in the Annex to this Resolution.

---

[1] CCP.I-TIC /doc. 1991/10 rev.1

2. That the CITEL Secretariat, with the Chair of PCC.I and the Rapporteurship of this subject, will coordinate this event and agenda with the ITU.

3. To encourage PCC.I members to participate in this Workshop.

4. That this Seminar shall be held without using the financial resources of CITEL.

ANNEX TO RESOLUTION PCC.I/RES. 166 (XVI-10)

DRAFT AGENDA

ITU AND CITEL REGIONAL CYBERSECURITY CAPACITY BUILDING WORKSHOP FOR THE AMERICAS

"International Cooperation for Building a Culture of Hemispheric Cybersecurity"

1 November 2010, Salta, Argentina (TBC)

08:00−09:00	**Meeting Registration and Badging (Online pre-registration required)**
09:00−09:20	**Meeting Opening and Welcoming Address**
	Opening Remarks: Host country representative ***Opening Remarks:*** CITEL ***Opening Remarks:*** International Telecommunication Union (ITU)
09:20−10:30	**Session 1: Understanding the Global and Hemispheric Cyber Threat Environment**
	Session Description**:** Confidence and security in using information and communication technologies are vital for building an inclusive, secure and global Information Society. The need to promote cybersecurity and protect critical infrastructures at the national, Regional and international level is generally acknowledged. This session shares an overview of the current cyber-threat landscape highlighting main threats and trends, and provides an insight into the challenges faced by countries, businesses and citizens in managing their every-day lives in this new and constantly changing environment. It further explores how countries in the hemisphere can evaluate risks related to possible attacks, by knowing what assets are critical to their national context and what different stakeholders need to be involved. It also details Regional activities carried out by OAS entities – CITEL, CICTE, and REMJA. (15 minutes for ITU, 15 for CITEL, 15 for CICTE, and 15 for REMJA)
10:30−10:45	**Break**

10:45−12:15	**Session 2: Technical Standards and Trusted information Sharing for improved Hemispheric Cybersecurity, and to build a Culture of Hemispheric Cybersecurity**
	Session Description: Each country and Region has its own requirements and needs that are to be addressed taking in consideration given the specific national and Regional context. One part of this session presents some of the main activities of standards development organizations (SDOs), focusing on topics such as security architecture, cybersecurity, security management, identity management, security baseline for network operators, the Global Cybersecurity Information Exchange Framework (CYBEX) and the ICT Security Standards Roadmap initiated by ITU-T Study Group 17. As national public and private sector actors bring their own perspective to the relevant importance of issues, the role of Regional and international standards development bodies becomes increasingly important. The second part of this session will discuss partnerships and consider the role of national, Regional and international activities in this context. By providing an understanding of each party's roles and responsibilities in cybersecurity and participating in reciprocal information sharing, dedicated and functional partnerships can mitigate and reduce risk and implement a comprehensive approach to cybersecurity. Promoting a culture of cybersecurity is critical for each country. Close collaboration is needed among all relevant stakeholders. As such the work that has been done in ITU-D Study Group 2, Question 22/1, has been fundamental to educating stakeholders in this regard. The third part of this session will provide an overview of the work that has been done in Question 22, and the synergies among parties in the Region.
12:15−13:15	**Break**
13:15−15:00	**Session 3: Defining Sound Organizational Structures and Developing Incident Management Capabilities to facilitate Hemispheric Cyber-security**
	Session Description: A key activity for addressing hemispheric cybersecurity requires the establishment of watch, warning and incident response capabilities to prepare for, detect, manage, and respond to cyber incidents. Effective incident management requires consideration of funding, human resources, training, technological capability, government and private sector collaboration, and legal requirements. This session discusses best practices, organizational structures and related standards in the technical, managerial and financial aspects of establishing national, Regional and international watch, warning, and incident response capabilities. The first part of this session will elaborate on the requirements for establishing watch, warning and incident response capabilities to respond to cyber incidents. This will include a demonstration of how a country can attempt to defend their networks against hostile attacks. What kind of indications will they be experiencing on their networks, what tools can they use to detect the intrusion, what tools are useful in managing and and responding to the attack and what processes and procedures should the country have put in place beforehand. The second part of this session will highlight the work being done by the OAS to promote a hemispheric culture of cybersecurity, particularly through Computer Security Incident Response Teams (CSIRTs) development and human-capacity development.

15:15−15:30	**Break**
15:30−17:00	**Session 4: Capacity Building and International and Hemispheric Cooperation**
	Session Description: The realities of cyberspace make it clear that everyone has to work together. Responding effectively to cyber-threats requires resources, know-how and strong investments on capacity developments. A key element is bringing together all relevant stakeholders to address the common cybersecurity challenges and develop solid capacity building plans. This session examines possible mechanisms to build capacity in an effective manner, through collaboration and cooperation among all stakeholders at the national, Regional and international level, for enhanced hemispheric cybersecurity and includes a focus on the important role of the private sector. It also includes a focus on benchmarking study/stock-taking exercise to provide Member States in the Americas Region with information to allow them to contrast and compare various current policies that are being implemented across the hemisphere as embodied in United Nations General Assembly Resolution 64-211.
17:00−17:15	**Workshop Wrap-Up, and Stock-taking**