ORGANIZACION DE LOS ESTADOS AMERICANOS
ORGANIZATION OF AMERICAN STATES

Comisión Interamericana de Telecomunicaciones
Inter-American Telecommunication Commission

XVII MEETING OF PERMANENT CONSULTATIVE COMMITTEE I: TELECOMMUNICATIONS/ INFORMATION AND COMMUNICATION TECHNOLOGIES
November 2 to 5, 2010
Salta, Argentina

OEA/Ser.L/XVII.4.1
CCP.I-TIC/doc. 2013/10 rev. 1
1 November 2010
Original: English

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)
(Item on the Agenda: 4.3)
(Document submitted by the ITU)

CITEL, 1889 F ST. NW., WASHINGTON, D.C. 20006, U.S.A.
TEL: +1 202 458 3004 FAX: +1 202 458 6854 e-mail: citel@oas.org
Web page: http://citel.oas.org

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)

08:00−09:00	**Meeting Registration and Badging (Online pre-registration required)**
09:00−09:20	**Meeting Opening and Welcoming Address**
	Opening Remarks: National Communications Secretariat - Argentina, Hector Carril ***Opening Remarks:*** CITEL, Clovis Baptista ***Opening Remarks:*** International Telecommunication Union (ITU), Mario Maniewicz
09:20−11:00	**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. - Mr. Mario Maniewicz ITU, Policies and Strategies, - Mr. Wayne Zeuch, CITEL, on behalf of the Rapporteur for Cybersecurity and Vulnerability Assesment - Mr. Belisario Contreras, CICTE - Mr. Albert Rees, REMJA, Chairman of WG on Cybersecurity Crime (remote presentation)
11:00−11:30	**Break**

11:30−13:00	**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. 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. The second part of this session will discuss partnerships and consider the role of national, Regional and international activities in this context. It also addresses the global concerns with problems of non-interoperability of products and systems claiming conformity to standards, especially in the developing world, how this has been captured in Resolutions of high level ITU forums, the role of conformity and interoperability testing to help mitigate these problems, and initiatives of the ITU-T and D-sectors in collaboration with industry to address these issues. - Mr. William McCrum, Consultant, TSB ITU - Mr. Antonio Guimaraes (Anatel), Vice-Chair of ITU-T SG17 - Mr. Wayne Zeuch, CITEL, PCC.I Rapporteur for Standards, Conformity and Interoperability
13:00−14:15	**Break**
14:15−16:00	**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. 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. Additionally, the work being done by ITU-D on the promotion of the importance of establishing National CIRTs will be highlighted.

	Finally, this session will also highlight the work being done by the Inter-American Committee Terrorism (CICTE) of the Secretariat for Multidimensional Security (SMS) of the OAS, in accordance with the Inter-American Comprehensive Strategy to Combat Cyber Threats, to promote the creation and development of national Computer Security Incident Response Teams (CSIRTs) in the Americas. - Mr. Emiliano Colina, Chief of Telecommunications, Ministry of Defense, UY - Mr. Jorge J. Uya, Information Security Specialist (remote presentation) - Dr. David Probert, ITU Expert – National Cybersecurity Strategy. - Mr. Belisario Contreras - CICTE
16:00−16:15	**Break**
16:15−17:45	**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. 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. A part of this session will provide an overview of the work that has been done in Question 22, and the synergies among parties in Q22 on Capacity Building. - ITU-D Q22-Cybersecurity, James Ennis, State Department USA - ITU Capacity Building efforts on Cybersecurity, Dr. David Probert - Project Amparo, Eduardo Carozo, Director - OAS/CICTE Expert – Belisario Contreras
17:45−18:00	**Workshop Wrap-Up, and Stock-taking** **1. ITU, Sergio Scarabino** **2. CITEL, Clovis Baptista**