PCC.I/RES. 49 (IV-04)[1]

CYBERSECURITY

The IV Meeting of the Permanent Consultative Committee I: Telecommunication Standardization,

RECOGNIZING:

a) That ensuring the safety and security of networked information systems (cybersecurity) is a priority item for our hemisphere;

b) That ubiquitous and secure information networks play an important role for the critical infrastructure of all OAS Member States, their economies and their societies; and

c) That the next generation networks (NGNs) presently being designed and standardized can take into account technologies and techniques to ensure their robustness and harden their resilience to cyber attacks,

TAKING INTO CONSIDERATION:

a) That secure and efficient operation of the global telecommunications infrastructure is crucial to the welfare and development of all sectors of the economy and therefore is of vital interest to both governments and the private sector; and

b) The increasingly frequent and insidious number of cyber attacks on networks, institutions and users, which is causing all kinds of harm, especially those moral, economic and financial,

CONSIDERING:

a) That CITEL, CICTE (the Inter-American Committee Against Terrorism of the OAS) and REMJA (the Meeting of Justice Ministers or Attorneys General of the Americas) are working towards the development of a hemispheric-wide strategy for cybersecurity, as determined by the OAS General Assembly in Resolution AG/RES.1939(XXXIII-O/03);

b) The workshop held jointly by the Working Group on Advanced Network Technologies and Services and the Working Group on Standards Coordination on cybersecurity at the IV PCC.I Meeting in Quito, Ecuador, addressed the key issues of cybersecurity as related to CITEL; and

c) The important commitments undertaken by the Heads of State and Government of the Region, as expressed in the Nuevo Leon Declaration, including the encouragement of affordable access to information and communications technologies for all,

FURTHER CONSIDERING:

That CITEL, through its partnering with the private sector on issues in its areas of responsibility, and through its Work Plan for advanced network issues, and in particular cybersecurity and NGNs, can make

[1] CCP.I-TEL/doc.427/04 rev.2

an important contribution to both raising awareness of critical issues potentially impacting the Region and refining its work plans in these areas through facilitation of focused discussion and information sharing.

RESOLVES :

1. To approve the attached contribution of CITEL to the OAS Cybersecurity Strategy and forward it to the OAS Committee on Hemispheric Security for review and submission to the OAS General Assembly in June 2004.

2. To request the CITEL's Rapporteur on Cybersecurity and Critical Infrastructure matters to convey a copy of this Resolution to the CICTE/CITEL/REMJA Joint Working Group on Cybersecurity.

INVITES:

a) The Working Group on Advanced Network Technologies and Services and the Working Group on Standards Coordination to continue working on the issue of cybersecurity and to report back to PCC.I on their findings on this particular matter.

b) The Chairman of PCC.I to send a letter to the Chairman of the OAS Committee on Hemispheric Security attaching a copy of this Resolution.

ANNEX TO RESOLUTION PCC.I/RES.49 (IV-04)

CITEL: The Identification and Adoption of Technical Standards for a Secure Internet Architecture

An effective cyber security strategy must recognize that the security of the network of information systems that comprise the Internet requires a partnership between government and industry. Both the telecommunications and information technology industries and the governments of OAS Member States are seeking cost-effective comprehensive cybersecurity solutions. Security capabilities in computer products are crucial to the overall network security. However, as more technologies are produced and integrated into existing networks, their compatibility and interoperability -- or the lack thereof -- will determine their effectiveness. Security must be developed in a manner that promotes the interweaving of acceptable security capabilities with the overall network architecture. To achieve such integrated, technology-based cybersecurity solutions, network security should be designed around international standards developed in an open process.

The development of standards for Internet security architecture will require a multi-step process to ensure that adequate agreement, planning, and acceptance is achieved among the various governmental and private entities that must play a role in the promulgation of such standards. Drawing upon the work of such standards development organizations as the Standardization Sector of the International Telecommunication Union (ITU-T), CITEL is identifying and evaluating technical standards to recommend their applicability to the Americas region, bearing in mind that the development of networks in some of the OAS Member States has suffered some delays, which implies that for those countries, the achievement of a certain degree of quality for their networks will be important to fully realize adequately secure information exchange systems. To expedite its work, CITEL and the ITU-T organized a joint workshop on Cybersecurity in March 2004. CITEL is also establishing liaisons with other standards bodies and industry fora to obtain the participation and feedback of those parties.

The identification of cyber security standards will be a multi-stepped process. Once CITEL's evaluation of existing technical standards is completed, it will recommend the adoption of standards of particular importance to the region. It will also, on a timely and ongoing basis, identify obstacles to implementation of those security standards in the networks of the region, and possible appropriate action that may be considered by Member States.

The development of technical standards is not a "one-size-fits-all" endeavor. CITEL will evaluate regional approaches to network security, deployment strategies, information exchange, and outreach to the public and the private sector. As part of this effort CITEL will identify resources for best practices for network communication and technology-based infrastructure protection. This process will require that CITEL review the objectives, scopes, expertise, technical frameworks and guidelines associated with available resources in order to determine their applicability within the Americas region to determine which ones are most appropriate. CITEL will continue to work with Member States to assist them for the most appropriate and effective implementation.

CITEL's contribution to the cyber security strategy will take a prospective approach and seek to foster information sharing among Member States to promote secure networks. It will identify and evaluate technical issues relating to standards required for security of future communications networks across the region, as well as existing ones. This task will draw primarily on the work of ITU-T. Through CITEL, other existing standards-setting bodies, will also be considered, as appropriate. Ultimately, CITEL will highlight security standards of particular importance and recommend that Member States endorse those standards. It is also important to highlight the crucial role of CITEL in promoting capacity building and training programs so as to to advance the process of spreading technical and practical information related to cybersecurity issues.

CITEL recognizes that, although the first priority must focus on public policies which will bring the benefits of telecommunications and information technologies to all citizens of the OAS Member States, strengthening the private/public partnership that will result in the wide scale adoption of a framework of technical standards that help secure the Internet will require communication and cooperation among and within the communities that are stakeholders in this partnership. CITEL will foster cooperation among Member States on aspects related to network security by helping Administrations adopt policies and practices that encourage network and service providers to implement technical standards for secure networks. The new edition of the Blue Book – "Telecommunications Policies for the Americas", a joint publication of CITEL and ITU, will include a chapter on cybersecurity. CITEL will also foster dialogue within the relevant technical and governmental communities regarding work on network and cyber security through joint seminars with the ITU on Security standards. The actions of CITEL may also include matters relating to telecommunications policies, practices, regulations, economic aspects and the responsibilities of the users, all within the legal framework within which the telecommunications services operates, and within the duties and responsibilities of CITEL.