PCC.I/RES.62 (V-04) [1]

CITEL CYBER SECURITY UPDATE

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

CONSIDERING:

a) The recent adoption by the XXXIV Meeting of the General Assembly of the OAS on June 8, 2004 of a comprehensive Inter – American Strategy to combat threats to cybersecurity; and

b) The continuing importance of fostering secure information and communication infrastructure to all OAS Members States, their economies and their societies,

NOTING:

a) That the ITU-T will hold a cybersecurity symposium to address global standardization concerns about security in information and communications systems on October 4, 2004, the day before the World Telecommunication Standardization Assembly (WTSA) convenes;

b) That CITEL PCC.I wishes to draw the attention of the Inter-American Committee against Terrorism (CICTE) and the Meeting of Ministers of Justice or Ministers or Attorneys General of the Americas (REMJA) to this symposium which is open to all. More information is contained on the Website: itu.int/ITU-T/worksem/cybersecurity.

FURTHER NOTING:

a) That CITEL PCC.I has endorsed by resolution PCC.I/RES. 45 (IV-04) a Coordinated Standard Document for "Security Architecture for Systems Providing End-to-End Communications" (ITU-T Rec. X.805) which defines a network security architecture for providing end-to-end network security. The architecture addresses security concerns for the management, control, and use of network infrastructure, services and applications. It provides a comprehensive, top-down, end-to-end perspective of network security and can be applied to network elements, services, and applications in order to detect, predict, and correct security vulnerabilities. Recommendation X.805 logically divides a complex set of end-to-end network security-related features into separate architectural components. This separation allows for a systematic approach to end-to-end security that can be used for planning of new security solutions as well as for assessing the security of the existing networks; and

b) That PCC.I has endorsed by resolution PCC.I/RES. 46 (IV-04) a Coordinated Standard Document for "Security Architecture for IP" (IETF RFC 2401) which addresses security at the IP Layer through the use of cryptographic and protocol security mechanisms. This security architecture, referred to as IPsec, provides security services by enabling a system to select required security protocols, determine the algorithms to use for services, and put in place any cryptographic keys required to provide the requested services. IPsec can be used to protect one or more "paths" between a pair of hosts, between a pair of security gateways, or between a security gateway and a host. IPsec is not an overall Security Architecture for the Internet; it addresses security only at the IP layer, provided through the use of a combination of cryptographic and protocol security mechanisms,

---

[1] CCP.I-TEL/doc.526/04 rev.1

RESOLVES:

To continue its efforts to identify telecommunication network vulnerabilities, to adopt technical standards to enhance the security of the telecommunication networks of the region and to investigate mitigation and response strategies to secure the regional critical telecommunications infrastructure. This will be accomplished through close private-public sector partnerships.

INVITES THE CHAIRMAN OF PCC.I:

To send a letter to the Chairman of the OAS Committee on Hemisphere Security that includes at least:

- A copy of this resolution
- Document PCC.I-TEL/doc.511/04 regarding the Cybersecurity Symposium
- Standard Coordination Documents endorsed, including an explanation of its objectives
- Work plan of the Working Group on Standards Coordination
- Work plan of the Study Question II of the Working Group on Advanced Network Technologies and Services: Cyber Security and Critical Infrastructure.