PCC.I/REC. 12 (XIX-11) [1]

GUIDELINES FOR THE FORMATION OF COMPUTER SECURITY INCIDENT RESPONSE TEAMS (CSIRTs)

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

CONSIDERING:

a) That in Resolution AG/RES. 2681 (XLI-O/11), “Increasing Access to Telecommunications and Information and Communication Technologies through Strengthening of the Inter-American Telecommunication Commission,” operative paragraph 1, the General Assembly resolves to renew its call on the Inter-American Telecommunication Commission (CITEL) to continue to collaborate closely with Member States in order to exchange best practices on policy, technologies, and national strategies on telecommunications/information and communication technologies (telecommunications/ICTs) and to promote even more vigorously the use of all appropriate media to serve rural, isolated, and underserved areas;

b) That the Working Group on Deployment of Technologies and Services of the Permanent Consultative Committee I: Telecommunications/ICT has a mandate to produce and recommend methodologies and best-practices for cyber security;

c) That confidence and security in the use of telecommunications/ICTs are highly important in creating the Information and Knowledge-based Society, as a result of which the countries of the region, especially the developing countries, require an ongoing exchange of experiences and best practices for the formulation of national, regional, and international policies in areas such as cyber security;

d) That the dissemination, knowledge, and attention to the issue of information security must be strengthened in the different Latin America and the Caribbean countries, especially in the private sphere of companies and civil society organizations; and

e) That guidelines are needed for the formation of Computer Security Incident Response Teams (CSIRT) within organizations (companies, institutions, etc.) of the different productive sectors of any country, including governmental entities,

RECOGNIZING:

a) That in Resolution 58 (Johannesburg, 2008), “Encourage the creation of national computer incident response teams, particularly for developing countries,” of the World Telecommunication Standardization Assembly of the International Telecommunication Union, the Member States are invited to consider the creation of a national Computer Incident Response Team (CSIRT) as a high priority;

b) That in Resolution 69 (Hyderabad, 2010), “Creation of national computer incident response teams, particularly for developing countries, and cooperation between them,” of the World Telecommunication Development Conference of the International Telecommunication Union, the Member States are invited to establish CSIRTs where necessary;

[1] CCP.I-TIC/doc.2482/11

c) That the Inter-American Committee against Terrorism (CICTE) of the Organization of American States (OAS) has a "Cyber Security" program, whose objective is to help Member States establish national "alert, watch, and warning" teams, also known as Computer Security Incident Response Teams (CSIRT),

BEARING IN MIND:

a) That there is a need to continue to strengthen bilateral, subregional, regional, and international cooperation mechanisms, in keeping with the principles enshrined in the OAS Charter, to address, prevent, and combat in an integral and effective manner transnational organized crime, human smuggling, terrorism, kidnapping, criminal gangs, and technology-related crimes, including cyber crime, since in some cases these may impact social, economic, political development, and legal and institutional systems;

b) That major challenges have arisen from the increasing digitization of the economy and society. SPAM, hacking of private information, and theft constitute some of the damage done to organizations and institutions by criminals and terrorists, especially those in countries without the institutional capacity for self-protection;

c) That to counteract these problems, one of the most widely used mechanisms is to have in place a group in the company, service, and/or country with the capacity to handle network security incidents,

RECOMMENDS:

1. That the Member States take note of the urgent need to establish Computer Security Incident Response Teams (CSIRT) as an element necessary to build confidence and security in the use of telecommunications/ICT as a pillar in creating the Information and Knowledge-based Society.

2. That the Member States utilize the public policy tools available to them to promote the creation of these teams, following the specific recommendations for their implementation and launch.

3. That the Administrations disseminate at the different levels (company, service, and/or country) information related to the need to create CSIRTs as a necessary tool for response to these incidents.

4. That the Member States of CITEL consider taking into account the following reference documentation when establishing national CSIRTS:

   a. The recently completed PCC.I document (CCP.I-TIC/doc.2342/11) on "Best Practices for National Cybersecurity: Building a National Computer Security Incident Management Capability";
   b. The three National Case Studies (Argentina, Dominican Republic, Venezuela) found in Chapters 1-3 of Appendix 2 in the Technical Notebook 4 "Cybersecurity";
   c. The Case Study from Mexico (CCP.I-TIC/doc.2334/11), "Guidelines for the Formation of Computer Security Incident Response Teams (CSIRTs) - (to be added in Chapter 4 of Appendix 2 in Technical Notebook 4 "Cybersecurity")

INSTRUCTS THE SECRETARIAT OF CITEL:

To forward this Recommendation to the CITEL Member States and to the CICTE Secretariat for its information.