Question 22/1: Securing information and communication networks: best practices for developing a culture of cybersecurity

1 Statement of the situation

in view of

a) The explosive growth in the deployment and use of information and communication technology (ICT) networks.

b) The need to ensure the security of these globally interconnected infrastructures if the potential of the information society is to be achieved.

c) The growing recognition at the national, regional and international levels of the need to develop and promote best practices, standards, technical guidelines and procedures to reduce vulnerabilities of and threats to ICT networks.

d) The need for national action and international cooperation to build a global culture of cybersecurity that includes national coordination, appropriate national legal infrastructures, watch, warning and recovery capabilities, government/industry partnerships, and outreach to civil society and consumers.

e) The requirement for a multistakeholder approach to effectively make use of the variety of tools available to build confidence in the use of ICT networks.

considering

a) That UN General Assembly Resolution 57/239, "Creation of a global culture of cybersecurity" invites Member States "to develop throughout their societies a culture of cybersecurity in the application and use of information technology".

b) That the Geneva Declaration of Principles indicates that "A global culture of cybersecurity needs to be promoted, developed and implemented in cooperation with all stakeholders and international expert bodies" and the Action line C5 of the Geneva Plan of Action encourages sharing best practices and the Tunis Agenda reaffirms the necessity for a global culture of cybersecurity.

c) That, consistent with its mandate, ITU should play a role in bringing together Member States, Sector Members and other experts to share experiences and expertise for securing ICT networks.

d) That developing countries face unique challenges in developing security policies and approaches appropriate to their circumstances.

e) That there exist considerable expertise and experience about network security among ITU Member States and Sector Members, within the current related work programmes in ITU-T, particularly Study Group 17, and in the ITU Strategic Planning Unit (SPU), within other international organizations, and among national and international private-sector bodies.

f) That Member States would benefit from a report detailing the various resources, strategies and tools available to build confidence in the use of ICT networks and the role of international cooperation in this regard.

2 Question for study

a) To survey, catalogue, describe and raise awareness of:

– the principal issues faced by national policy-makers in working with all stakeholders to build a culture of cybersecurity;

– the principal sources of information and assistance related to building a culture of cybersecurity;

– successful best practices employed by national policy-makers in working with all stakeholders to organize for cybersecurity and develop a culture of security;

– the unique challenges faced by developing countries in addressing the security of networks and the best practices for addressing these challenges.

b) To examine best practices for the establishment and operation of watch, warning and incident response and recovery capabilities that may be used by Member States to establish their own national capabilities.

3 Expected output

A report or reports to the membership on the issues identified in section 2 above. The report or reports in question will reflect that secure information and communication networks are integral to building of the information society and to the economic and social development of all nations. Cybersecurity challenges include potential unauthorized access to, destruction of, and modification of information transmitted on ICT networks. However, the consequences of such challenges can be mitigated by increasing awareness of cybersecurity issues and sharing successful best practices employed by policy-makers working with other stakeholders. In addition, a culture of cybersecurity can promote trust and confidence in these networks, stimulate secure usage, ensure protection of data and privacy while enhancing access and trade, and enable nations to better achieve the economic and social development benefits of the information society.

4 Timing

This study is proposed to last four years, with preliminary status reports to be delivered on progress made after 12, 24, and 36 months.

5 Proposers

CITEL administrations

6 Sources of input

a) Contributions from Member States and Sector Members.

b) Relevant work currently being undertaken in ITU-T, ITU-R and SPU.

c) Relevant international organizations, such as OECD and the Council of Europe.

d) Relevant non-governmental organizations concerned with the promotion of cybersecurity and a culture of security.

e) Surveys of ITU members' experiences, as appropriate.

f) Worldwide websites of national cybersecurity authorities.

g) Other sources, as appropriate.

7 Target audience

	Developed countries	Developing countries	LDCs
Telecom policy-makers	*	*	*
Telecom regulators	*	*	*
Service providers/operators	*	*	*
Manufacturers	*	*	*

.

a) Target audience

National policy-makers and Sector Members, and other stakeholders involved in or responsible for cybersecurity activities, especially those from developing counties.

b) Proposed methods for the implementation of the results

The study programme being focused on gathering information and best practices is intended to be informative in nature and can be used to raise awareness for Member States and Sector Members of the issues of cybersecurity and to draw attention to the information, tools and best practices available, the results of which may be used in conjunction with BDT-organized seminars and workshops.

8 Proposed methods of handling the Question or issue

Given the nature of the proposed Question, the potential quantity of information sources required and the time that will have to be devoted to identifying solutions to the issues at hand, it is considered necessary that the Question be addressed within a study group over a four-year study period (with submission of interim results).

9 Coordination

Coordination with ITU-T, in particular SG 17, as well as with ongoing SPU activities is necessary. In addition, given the existing level of technical expertise on the issue in ITU-T SG 17, all documents (questionnaire, interim reports, draft final reports, etc.) should be sent to SG 17 for comment and input prior to being submitted to the full ITU-D SG for comment and approval.

_____