World Telecommunication Development Conference (WTDC-14)
Dubai, 30 March – 10 April 2014

Addendum 6 to
Document WTDC14/22-E
4 February 2014
Original: English

SOURCE: United States of America

TITLE: Proposed modifications to Question 22-1/1

Background

Information and communication technologies (ICTs) are integral to the economic and social development of all nations as well as to the development of the information society. Security is an essential element of the operation and use of ICTs and requires that all persons involved be aware of security and take action appropriate to their role. As the use of ICT continues to grow, the multiple aspects of cybersecurity and combating the transmission of email spam continues to be a priority among members. During the last four years, the ITU-D's Question 22-1/1 and Programme 2 both continued to work in this area. Q 22-1/1 developed products and materials to support countries in developing national cybersecurity capabilities, to convene experts, and to contribute to ongoing information sharing on best practices. The Question also identified key areas of common concern as well as gaps, based on contributions to a compendium and a survey, respectively. Programme 2 undertook many activities that offer development assistance to members and encourage cooperation among members.

Discussion

The United States believes that, given the dynamic nature of the cybersecurity challenge and new means to address it, it is important to maintain the Question text current with an achievable set of goals that meet the priority needs of developing countries. We also believe that it is highly desirable to build on the linkage and collaboration between the Question and Programme 2. CITEL is of the same belief.

Proposal

USA/22/6 Objective(s): 3

The United States proposes that Question 22-1/1 be modified according to the text in the attached document.

Contact: Name/Organization/Entity: Paul Najarian, United States of America
Phone number: +1 202 6477847
E-mail: najarianpb@state.gov

BDT 2/12/14 3:50 PM
Style Definition: Normal: Font:+Theme Body

BDT 2/12/14 3:50 PM
Style Definition: Footnote Reference,Appel note de bas de p,Footnote Reference/,Footnote symbol,Ref,de nota al pie: Font:+Theme Body

BDT 2/12/14 3:50 PM
Style Definition: Footnote Text Char,DNV-F Char Char,DNV-FT Char: Font:+Theme Body, 12 pt

BDT 2/12/14 3:50 PM
Style Definition: Annex_title: Font:+Theme Body

BDT 2/12/14 3:50 PM
Style Definition: Heading_b: Font:+Theme Body

BDT 2/12/14 3:50 PM
Style Definition: Page Number: Font:+Theme Body

BDT 2/12/14 3:50 PM
Style Definition: Footnote Text Char2,ACMA Footnote Text Char1,ALTS FOOTNOTE Char1,Footnote Text Char1 Char1,Footnote Text Char Char1 Char1,Footnote Text Char4 Char Char Char1,Footnote Text Char1 Char1 Char1 Char Char1,Footnote Text Char Char1 Char1 Char Char Char1

BDT 2/12/14 3:50 PM
Style Definition: FirstFooter: Check spelling and grammar, Not All caps, Space Before: 2 pt, Allow hanging punctuation, Adjust space between Latin and Asian text, Adjust space between Asian text and numbers, Font Alignment: Auto, Tabs:Not at 4.13" + 6.69"

BDT 2/12/14 3:50 PM
Style Definition: Special Footer: Check spelling and grammar, Not All caps, Justified, Tabs: 0.39", Left + 0.79", Left + 1.18", Left + 1.58", Left + 1.97", Left

Terms of reference for Question 22-1/1

Question 22-1/1: 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 technologies (ICT);

b) the fact that cybersecurity remains a concern of all stakeholders;

c) the need to endeavor to ensure the security of these globally interconnected infrastructures if the potential of the information society is to be achieved;

d) 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;

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

f) the requirement for a multi-stakeholder approach to effectively make use of the variety of tools available to build confidence in the use of ICT networks,

g) the fact that the 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";

h) the fact that best practices in cybersecurity must protect and respect the rights of privacy and freedom of expression as set forth in the relevant parts of the Universal Declaration of Human Rights, the Geneva Declaration of Principles, and other relevant international human rights instruments;

i) the fact 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", the Geneva Plan of Action encourages sharing best practices and taking appropriate action on spam at national and international levels, and the Tunis Agenda reaffirms the necessity for a global culture of cybersecurity, particularly Action Line C5 (building confidence and security in the use of ICTs);

j) the fact that the ITU was requested by the WSIS Tunis 2005 in its agenda for the implementation and follow up to be the lead facilitator/moderator for Action Line C5 "**Building confidence and security in the use of ICTs**". ITU-T, ITU-R, ITU-D and General Secretariat based on such responsibility and in response to relevant resolutions adopted by the WTDC (Doha, 2006 & Hyderabad, 2010), by the Plenipotentiary (Antalya, 2006 & Guadalajara, 2010) as well as by WTSA (Johannesburg, 2008 & Dubai, 2012), carried out many studies in order to improve cybersecurity,

BDT 2/12/14 3:50 PM
Formatted: Font:11 pt

BDT 2/12/14 3:50 PM
Formatted: Widow/Orphan control

Editor 9/24/13 7:33 PM
Deleted: technology networks

BDT 2/12/14 3:50 PM
Formatted: Justified

Editor 9/24/13 7:47 PM
Deleted: networks

BDT 2/12/14 3:50 PM
Formatted: Font:Not Italic

Editor 1/23/14 2:48 PM
Deleted: that criminal attacks on cybersecurity are growing, and no efficient measures were able to stop them

BDT 2/12/14 3:50 PM
Deleted: ;

BDT 2/12/14 3:50 PM
Deleted: -

Editor 9/20/13 11:04 AM
Deleted: unique

BDT 2/12/14 3:50 PM
Deleted: the

BDT 2/12/14 3:50 PM
Deleted:),

Editor 9/24/13 6:44 PM
Deleted: with the expectation of updating them in Hyderabad 2010 this year

Micaela Klein 9/27/13 11:28 AM
Deleted: P

BDT 2/12/14 3:50 PM
Deleted: PP

Micaela Klein 9/27/13 11:28 AM
Deleted: -06

Micaela Klein 9/27/13 11:28 AM
Deleted: -08

BDT 2/12/14 3:50 PM
Deleted: ;

k) WSIS outputs in both Geneva 2003 and Tunis 2005 called for building confidence and security in the use of ICTs.

l) that Resolution 45 [Rev. Dubai, 2014] of the World Telecommunication Development Conference supported the enhancement of cybersecurity amongst interested Member States;

m) that consistent with its mandate, ITU-D should play a role in bringing together Member States, Sector Members and other experts to share experiences and expertise for securing ICT networks;

n) the excellent results of Question 22-1/1 for the past study period that include numerous reports, and contributions from across the globe ;

o) that there have been various efforts to facilitate the improvement of network security by many experts across the globe;

p) that particularly least developed countries' governments, service providers and end-users face unique challenges in developing security policies and approaches appropriate to their circumstances;

q) that Member States and infrastructure operators would benefit from additional reports 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;

r) that spam continues to be a concern.

2 Question or issues for study

a) Discuss approaches and best practices for evaluating the impact of spam within a network, and to provide mitigation approaches that developing countries can use, taking into account existing standards and available tools;

b) Provide a view of current cybersecurity challenges, such as those facing service providers, based on available literature;

c) Continue to gather national experiences relating to cybersecurity from developing and developed countries, and to examine common themes within those experiences.

d) Continue to analyse results of the cybersecurity awareness survey taken in the last study period, and reissue an updated survey so as to measure progress over time;

e) Provide a compendium of relevant, ongoing cybersecurity activities being conducted by organizations, the private sector, and civil society at the national, regional, and international levels, in which developing countries and all sectors may participate;

f) Examine specific needs of persons with disabilities in coordination with other relevant Questions;

g) Examine means to assist least developed countries;

h) Take in national requirements and experience specifically in the area of child online protection, in coordination with other relevant activities;

i) Examine abuse of numbering issues that arise, in coordination with ITU-T SG 2.

BDT 2/12/14 3:50 PM
Formatted: Font:11 pt

BDT 2/12/14 3:50 PM
Deleted:

BDT 2/12/14 3:50 PM
Formatted: Font:Not Italic

BDT 2/12/14 3:50 PM
Deleted: ;

Editor 9/24/13 6:47 PM
Deleted: (

Editor 9/24/13 6:48 PM
Deleted: Hyder

CITEL 10/27/13 8:06 AM
Deleted: a

Editor 9/24/13 6:48 PM
Deleted: bad

BDT 2/12/14 3:50 PM
Deleted: ,

Editor 9/24/13 6:48 PM
Deleted: 2010

Editor 9/24/13 6:47 PM
Deleted:)

Editor 9/24/13 6:49 PM
Deleted: entitled,

BDT 2/12/14 3:50 PM
Deleted: /1 entitled

Editor 9/24/13 6:49 PM
Deleted: "Report on Best Practices for a National Approach to Cybersecurity: Building Blocks for Organizing National Cybersecurity Efforts", in its final report for the period 2006-2009, as shown in Document 1/249(Rev.1) for this Question 2009, justified the continuation of this Question for another new cycle with different orientations taking into consideration the needs of developing countries

Editor 9/24/13 6:50 PM
Deleted: ,

BDT 2/12/14 3:50 PM
Deleted: ,

Editor 9/24/13 6:50 PM
Deleted: including the work of Member States and Sector Members in standard ... [1]

BDT 2/12/14 3:50 PM
Deleted:

Editor 9/24/13 6:50 PM
Deleted: Development Sector in its ca ... [2]

Editor 9/24/13 6:51 PM
Deleted: developing

Editor 9/24/13 7:36 PM
Deleted: .

BDT 2/12/14 3:50 PM
Formatted: Widow/Orphan control

3 Expected output

1 Reports to the membership on the issues identified in section 2 a) i) above. The 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 as well as countering and combating spam. However, the consequences of such challenges can be mitigated by increasing awareness of cybersecurity issues, establishing effective public-private partnerships, and sharing successful best practices employed by policy-makers and businesses and through collaborating 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.

2 Educational materials for use in workshops, seminars, etc.

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 Proposer

United States of America, CITEL

6 Sources of input

a) Member States and Sector Members.

b) Relevant ITU-T and ITU-R Study Group work.

c) Relevant outputs of international and regional organizations.

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

e) Surveys, online resources.

f) Other sources, as appropriate.

7 Target audience

	Developed countries	Developing countries[3]
Telecom policy makers	Yes	Yes
Telecom regulators	Yes	Yes
Service providers/ operators	Yes	Yes

[3] These include the least developed countries (LDCs), small island developing states (SIDS), landlocked developing countries (LLDCs) and countries with economies in transition.

BDT 2/12/14 3:50 PM Formatted ... [3]
BDT 2/12/14 3:50 PM Deleted: a) . Update the output of ... [4]
BDT 2/12/14 3:50 PM Formatted ... [5]
BDT 2/12/14 3:50 PM Formatted ... [6]
GPiedras 11/7/13 8:49 PM Deleted: b
BDT 2/12/14 3:50 PM Deleted: 2b
GPiedras 11/7/13 8:49 PM Deleted: -v)
BDT 2/12/14 3:50 PM Deleted: .
BDT 2/12/14 3:50 PM Formatted ... [7]
BDT 2/12/14 3:50 PM Formatted ... [8]
BDT 2/12/14 3:50 PM Formatted ... [9]
BDT 2/19/14 8:50 AM Deleted: ITU-D Study Group 1, CITEL ... [10]
BDT 2/12/14 3:50 PM Formatted ... [11]
Editor 9/24/13 7:52 PM Deleted: , including ISO and OECD
BDT 2/12/14 3:50 PM Formatted ... [12]
BDT 2/12/14 3:50 PM Deleted: .
BDT 2/12/14 3:50 PM Formatted ... [13]
BDT 2/12/14 3:50 PM Formatted ... [14]
BDT 2/12/14 3:50 PM Formatted Table ... [15]
BDT 2/12/14 3:50 PM Formatted ... [16]
BDT 2/12/14 3:50 PM Formatted ... [17]
BDT 2/12/14 3:50 PM Formatted ... [18]
BDT 2/12/14 3:50 PM Formatted ... [19]
BDT 2/12/14 3:50 PM Formatted ... [20]
BDT 2/12/14 3:50 PM Formatted ... [21]
BDT 2/12/14 3:50 PM Formatted ... [22]
BDT 2/12/14 3:50 PM Deleted: ———————
BDT 2/12/14 3:50 PM Deleted: . This includes
BDT 2/12/14 3:50 PM Formatted ... [23]

Manufacturers	Yes	Yes

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 focuses on gathering information and best practices. It 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

The Question will be addressed within a study group over a four-year study period (with submission of interim results), and will be managed by a Rapporteur and Vice-Rapporteurs. This will enable Member States and Sector Members to contribute their experiences and lessons they have learned with respect to cybersecurity.

9 Coordination

Coordination with ITU-T, ITU-D Question 20-1/1 on Persons with Disabilities, as well as other relevant organizations, including FIRST, AP-CERT, OAS CICTE, OECD, RIRs, NOGs, M3AAWG, and others. Given the existing level of technical expertise on the issue in these groups, all documents (questionnaires, interim reports, draft final reports, etc.) should be sent to them for comment and input prior to being submitted to the full ITU-D Study Group for comment and approval.

10 BDT Programme link

BDT Programme 2 shall facilitate exchange of information and make use of the output, as appropriate, to satisfy program goals and the needs of Member States.

BDT 2/12/14 3:50 PM
Formatted: Font:11 pt

BDT 2/12/14 3:50 PM
Formatted: Font:12 pt

BDT 2/12/14 3:50 PM
Formatted: Line spacing: multiple 1.15 li

BDT 2/12/14 3:50 PM
Deleted: .

BDT 2/12/14 3:50 PM
Formatted: Heading 2

BDT 2/12/14 3:50 PM
Formatted: Justified

BDT 2/12/14 3:50 PM
Formatted: Heading 2

BDT 2/12/14 3:50 PM
Formatted: Justified

BDT 2/12/14 3:50 PM
Formatted: Widow/Orphan control

BDT 2/12/14 3:50 PM
Formatted: Justified

BDT 2/12/14 3:50 PM
Deleted: Study Group 1

BDT 2/12/14 3:50 PM
Deleted:

BDT 2/12/14 3:50 PM
Formatted: Widow/Orphan control

Editor 9/24/13 6:53 PM
Deleted: in particular Study Group 17 or its successor,

Editor 9/24/13 6:54 PM
Deleted: ITU-T Study Group 17,

Editor 9/24/13 6:55 PM
Deleted: SG 17

BDT 2/12/14 3:50 PM
Formatted: Widow/Orphan control

BDT 2/19/14 8:52 AM
Deleted: ITU-D

BDT 2/19/14 8:52 AM
Formatted: Justified

Page 3: [1] Deleted	Editor	9/24/13 6:50 PM

including the work of Member States and Sector Members in standards-setting activities in the ITU-T and in the development of best practices reports in ITU-D; by the ITU Secretariat in the Global Cybersecurity Agenda (GCA); and by the ITU-

Page 3: [2] Deleted	Editor	9/24/13 6:50 PM

Development Sector in its capacity-building activities in Programme 3

Page 1: [3] Formatted	BDT	2/12/14 3:50 PM

Font:11 pt

Page 4: [4] Deleted	BDT	2/12/14 3:50 PM

a) Update the output of the past cycle taking into consideration the needs of developing countries and reflecting the results achieved by the ITU as a whole (the relevant outputs of ITU-T SG 17/T and SG 13/T, the relevant output of the specialized programme for cybersecurity in the BDT, the General Secretariat activities as a follow-up to Action Line C5 and the output of the High Level Expert Group (HLEG) which was supported by all developing countries experts) as well as progress achieved on the subject by ISO/IEC. This revision shall take into consideration also the progress achieved by the project "IMPACT", FIRST, and similar projects where many developing countries are member now.

b) During the next study period, to expand upon the information contained in the Best Practices Report Phase I dealing with: 1) developing a national strategy for cybersecurity; 2) developing public/private partnerships; 3) creating national cyber incident management capability developing incident watch, warning and response and recovery mechanisms; 4) developing a culture of awareness; and 5) identifying best practices to protect against spam malware and other cyberthreats:

   i) With respect to developing a national strategy for cybersecurity, a) to develop models for national cybersecurity management; b) to identify organizational models that countries have followed and techniques they have used in developing a national strategy, with lessons learned, in particular of these models used by OECD, or any recommended model by Europe as a whole.

   ii) With respect to public/private partnerships, to elaborate on 1) the principles for sound public/private partnerships; 2) various structural models for achieving sound public/private partnerships; and 3) the concept of risk mitigation with respect to public/private partnerships and the relative roles of each.

   iii) With respect to creating national cyber incident management capability, to elaborate on the development of watch, warning and response and recovery mechanisms, and the establishment of national computer security incident response teams.

iv) Taking into consideration the existing studies in ITU-T SG 17 on enlarging these national centres to cover all matters related to cybersecurity in general and not to be limited to the Internet only, as well as the product of the relevant ITU-D programme regarding CIRT, preferably responding to regional needs of the six existing BDT regions, not forgetting that a single model for all developing countries might be the best practice in this domain[1].

v) With respect to developing a culture of cybersecurity awareness, to collect ideas from all sources on how countries, businesses and expert groups are educating and encouraging individuals and entities on the subject of cybersecurity, including child online protection, and the cybersecurity needs of persons with disabilities.

vi) With respect to identifying best practices and strategies to protect against spam and malware: 1) to examine and identify national consumer and business education efforts to help build user confidence through the prevention and mitigation of spam and malware; 2) to examine the role that governments and non-governmental organizations have in promoting the prevention of spam and malware, including consideration of their respective best practices, guidelines and codes of conduct; 3) to examine the methods used to educate end-users of the risks associated with phishing schemes, botnets, viruses and other malicious content that may be contained in spam, as well as preventative measures employed; and, 4) to examine perspectives on mechanisms used to improve cybersecurity, and to identify what information, capabilities, tools and mechanisms are available to businesses and other end users.

vii) To conduct surveys, as appropriate, in the areas identified above, in order to identify steps taken by countries, businesses and expert bodies.

viii) As a result of the surveys conducted, create a compendium of all relevant national and/or regional practices in this domain, including all responses and relevant information.

ix) To conduct a benchmarking study/stocktaking exercise to provide Member States with information to allow them to contrast and compare various current policies that are in implementation in ITU Member States.

x) To consider all available information on these topics from a variety of sources, including relevant stakeholders.

---

[1] NOTE – Pending approval by the WTDC Hyderabad 2010 on the proposed new resolution which encourages developing countries to create national computer incident response teams (CIRT), this Question shall assist in addressing this resolution if approved.

c) Use the Best Practices Report, plus other relevant material, to develop course materials on the topics identified in 2b) i)-v) above to assist in the analysis of national cybersecurity strategies and the planning of hands-on training programmes. Such course materials could be used on their own or as part of expert workshops and other forums.

d) Based on contributions submitted, to assemble a volume of country case studies for informational purposes describing the current status of countries' cybersecurity efforts, and their cybersecurity policies.

e) Develop a framework to be pursued and implemented under Programme 2 in BDT for increasing awareness by developing countries regarding cybersecurity, covering all levels, national, regional and international in particular:

- the role of the government(s), including the national centre for cybersecurity;
- the role of the intergovernmental groups for national, regional and international;
- the role of the non-governmental groups for national, regional and international;
- etc.

In order for the BDT to carry out a plan of action for raising awareness of cybersecurity on all levels in developing countries.

f) this Question may take a partial role on the implementation of the new revised Resolution 45[2].

Page 4: [5] Formatted **BDT** **2/12/14 3:50 PM**

Widow/Orphan control

Page 4: [6] Formatted **BDT** **2/12/14 3:50 PM**

Justified

Page 4: [7] Formatted **BDT** **2/12/14 3:50 PM**

Widow/Orphan control

Page 4: [8] Formatted **BDT** **2/12/14 3:50 PM**

Justified

Page 4: [9] Formatted **BDT** **2/12/14 3:50 PM**

Widow/Orphan control

Page 4: [10] Deleted **BDT** **2/19/14 8:50 AM**

[2] NOTE – This clause depends on the outcome on WTDC Hyderabad revisions to Resolution 45.

ITU-D Study Group 1, CITEL, Arab States

Page 4: [10] Deleted	BDT	2/19/14 8:50 AM

ITU-D Study Group 1, CITEL, Arab States

Page 4: [11] Formatted	BDT	2/12/14 3:50 PM

No widow/orphan control

Page 4: [12] Formatted	BDT	2/12/14 3:50 PM

Space After: 12 pt

Page 4: [13] Formatted	BDT	2/12/14 3:50 PM

Indent: Left: 0", First line: 0", Line spacing: multiple 1.15 li

Page 4: [14] Formatted	BDT	2/12/14 3:50 PM

Font:12 pt

Page 4: [15] Formatted Table	BDT	2/12/14 3:50 PM

Formatted Table

Page 4: [16] Formatted	BDT	2/12/14 3:50 PM

Line spacing: multiple 1.15 li

Page 4: [17] Formatted	BDT	2/12/14 3:50 PM

Font:12 pt

Page 4: [18] Formatted	BDT	2/12/14 3:50 PM

Line spacing: multiple 1.15 li, Keep with next

Page 4: [19] Formatted	BDT	2/12/14 3:50 PM

Font:12 pt

Page 4: [20] Formatted	BDT	2/12/14 3:50 PM

Line spacing: multiple 1.15 li

Page 4: [21] Formatted	BDT	2/12/14 3:50 PM

Font:12 pt

Page 4: [22] Formatted	BDT	2/12/14 3:50 PM

Line spacing: multiple 1.15 li

Page 4: [23] Formatted	BDT	2/12/14 3:50 PM

Font:9 pt