Geneva, 15 October 2013

|  |  |
| --- | --- |
| **Telecommunication StandardizationBureau** |  |
|  |  |

|  |  |  |
| --- | --- | --- |
| Ref:Tel:Fax: | **TSB Circular 57**COM 17/MEU+41 22 730 5866+41 22 730 5853 | - To Administrations of Member States of the Union |
| E-mail: | tsbsg17@itu.int | **Copy:**- To ITU-T Sector Members;- To ITU-T Associates;- To ITU-T Academia;- To the Chairman and Vice-Chairmen of Study Group 17;- To the Director of the Telecommunication Development Bureau;- To the Director of the Radiocommunication Bureau |

|  |  |
| --- | --- |
| Subject: | **Meeting of Study Group 17 with a view to approving draft new Recommendation ITU-T X.1208 in accordance with the provisions of Resolution 1, Section 9, of WTSA (Dubai, 2012), Geneva, 15-24 January 2014** |

Dear Sir/Madam,

1 At the request of the Chairman of Study Group 17, *Security*, I have the honour to inform you that this Study Group, which will meet from 15 to 24 January 2014, intends to apply the procedure described in Resolution 1, Section 9, of WTSA (Dubai, 2012) for the approval of the above-mentioned draft new Recommendation.

2 The title, summary and location of the draft new ITU-T Recommendation proposed for approval is found in **Annex 1**.

3 Any ITU Member State, Sector Member, Associate or Academic Institution aware of a patent held by itself or others which may fully or partly cover elements of the draft Recommendations proposed for approval is requested to disclose such information to TSB, in accordance with the Common Patent Policy for ITU-T/ITU-R/ISO/IEC.

Available patent information can be accessed on‑line via the ITU‑T website ([www.itu.int/ITU-T/ipr/](http://www.itu.int/itu-t/ipr/)).

4 Having regard to the provisions of Resolution 1, Section 9, I should be grateful if you would inform me by 2400 hours UTC **on 3 January 2014** whether your Administration assigns authority to Study Group 17 that this draft new Recommendation should be considered for approval at the Study Group meeting.

 Should any Member States be of the opinion that consideration for approval should not proceed, they should advise their reasons for disapproving and indicate the possible changes that would facilitate further consideration and approval of the draft new Recommendation.

5 If 70% or more of the replies from Member States support consideration for approval of this draft new Recommendation at the Study Group meeting, one Plenary session will be devoted **on 24 January 2014** to apply the approval procedure.

I accordingly invite your Administration to send a representative to the meeting. **The Administrations of Member States of the Union** are invited to supply the name of the head of their delegation. If your Administration wishes to be represented at the meeting by a recognized operating agency, a scientific or industrial organization or another entity dealing with telecommunication matters, the Director should be duly informed, in accordance with Article 19, No. 239, of the ITU Convention.

6 The agenda and all relevant information concerning the Study Group 17 meeting will be available from Collective letter 3/17.

7 After the meeting, the Director of TSB will notify, in a circular, the decision taken on this Recommendation. This information will also be published in the ITU Operational Bulletin.

Yours faithfully,

Malcolm Johnson
Director of the Telecommunication
Standardization Bureau

**Annex**: 1

ANNEX 1
(to TSB Circular 57)

**Summary and location of the text**

**Draft new Recommendation ITU-T X.1208 (X.csi)
(COM 17 – R 22)**

A cybersecurity indicator of risk to enhance confidence and security in the use of telecommunication/information and communication technology

Summary

Recommendation ITU-T X.1208 provides a list of potential indicators and describes a methodology used in computing a risk measure for that organization with respect to those cybersecurity indicators.

Recommendation ITU-T X.1208 is intended to help organizations that implement or operate a portion of the global infrastructure of information and communication technologies to evaluate their own cybersecurity capability and risk. These guidelines are intended to facilitate the decision making process within an organization on how to improve cybersecurity, how to lower their risks, and where they could/should invest resources to improve their cybersecurity.

\_\_\_\_\_