|  |  |  |
| --- | --- | --- |
| itu_logo | **International telecommunication union****Telecommunication Standardization Bureau** |  |
|  | Geneva, 21 October 2015 |
| Ref: | **TSB Circular 174**COM 17/MEU | - To Administrations of Member States of the Union |
| Tel: | +41 22 730 5866 |
| Fax: | +41 22 730 5853 |
| E-mail: | tsbsg17@itu.int  | **Copy:**- To ITU-T Sector Members;- To ITU-T Associates;- To ITU 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 Recommendations ITU‑T X.1247, X.1256, X.1257, X.1602, X.1642 and draft revised Recommendation ITU‑T X.1521, in accordance with the provisions of Resolution 1, Section 9, of WTSA (Dubai, 2012) Geneva, 23 March 2016** |

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 14 to 23 March 2016, intends to apply the procedure described in Resolution 1, Section 9, of WTSA (Dubai, 2012) for the approval of the above-mentioned draft revised and draft new Recommendations.

2 The titles, summaries and locations of the draft revised and draft new ITU-T Recommendations proposed for approval will be 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/ipr/](http://www.itu.int/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 2 March 2016** whether your Administration assigns authority to Study Group 17 that these draft new and revised Recommendations 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 revised or new Recommendations.

5 If 70% or more of the replies from Member States support consideration for approval of these draft new and revised Recommendations at the Study Group meeting, one Plenary session will be devoted **on 23 March 2016** 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 7/17.

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

Yours faithfully,

Chaesub Lee
Director of the Telecommunication
Standardization Bureau

**Annex**: **1**

ANNEX 1
(to TSB Circular 174)

**Summary and location of the texts**

**Draft new Recommendation ITU-T X.1247 (X.tfcmm), Technical framework for countering mobile messaging spam
COM 17 – R 50**

**Summary**

Mobile messaging spam is proliferating dramatically along with the fast development of mobile messaging services. Unfortunately, no single measure has proved to be the silver bullet against mobile messaging spam. Therefore, it is necessary to establish a practical framework for countering mobile messaging spam. Recommendation ITU-T X.1247 gives an overview of mobile messaging anti-spam processes, and proposes a technical framework for countering mobile messaging spam. Entity functions and processing procedures are specified in this framework. In addition, this Recommendation provides information sharing mechanisms against mobile messaging spam within the anti-spam domain and among anti-spam domains.

**Draft new Recommendation ITU-T X.1256 (X.authi), Guidelines and framework for sharing network authentication results with service applications
COM 17 – R 54**

**Summary**

With the surge of mobile devices and applications accessing the Internet, the network and the service environment are becoming increasingly complicated. As a result, there is a pressing need to simplify the user authentication mechanism to improve user experience and service quality.

Many standardization organizations including ITU-T have conducted a lot of research work on the unified authentication mechanism (i.e., single sign-on). However, all the current work is basically focused on unified authentication among the service applications, without considering the relationship with the network authentication.

From the network operator's perspective, users undergo some forms of network authentication when they access the network, however, when they log in again to request access to a service their initial network authentication is not reused anymore. When adopting an authentication results sharing mechanism between the service and the network, the service applications can identify a user by using the authentication results from the network. Such mechanism allows a user to be authenticated only once by the network and directly gain access to the service.

Recommendation ITU-T X.1256 develops guidelines for network operators and service providers to share network authentication results, and provides a framework for sharing minimum attributes across multiple services within an established trust relationship.

**Draft new Recommendation ITU-T X.1257 (X.iamt), Identity and access management taxonomy
COM 17 – R 55**

**Summary**

Recommendation ITU-T X.1257 develops a specification to ensure that necessary business meaning is assigned to IAM roles and permissions and that this business meaning is traceable and reference-able throughout IAM process lifecycle so that permissions can be efficiently assigned to user, separation of duties (SoD) controls successfully implemented across applications, and access review and reconciliation processes can be carried out efficiently.

**Draft revised Recommendation ITU-T X.1521 (X.cvss), Common vulnerability scoring system 3.0
COM 17 – R 49**

**Summary**

Recommendation ITU-T X.1521 on the common vulnerability scoring system (CVSS) provides an open framework for communicating the characteristics and impacts of information and communication technologies (ICT) vulnerabilities in the commercial or open source software used in communications networks, end user devices, or any of the other types of ICT capable of running software. The goal of the Recommendation is to enable ICT managers, vulnerability bulletin providers, security vendors, application vendors and researchers to speak from a common language of scoring ICT vulnerabilities.

**Draft new Recommendation ITU-T X.1602 (X.sfcse), Security requirements for software as a service application environments
COM 17 – R 52**

**Summary**

Recommendation ITU-T X.1602 analyses the maturity levels of software as a service (SaaS) application and proposes security requirements to provide a consistent and secure service execution environment for SaaS applications. These proposed requirements originate from cloud service providers (CSP) and cloud service partners (CSN) as they need a SaaS application environment to meet their demands on security. The requirements are general and independent of any service or scenario specific model (e.g. web services, or representational state transfer (REST)), assumptions or solutions.

**Draft new Recommendation ITU-T X.1642 (X.goscc), Guidelines for the operational security of cloud computing
COM 17 – R 53**

**Summary**

Recommendation ITU-T X.1602 analyses the maturity levels of software as a service (SaaS) application and proposes security requirements to provide a consistent and secure service execution environment for SaaS applications. These proposed requirements originate from cloud service providers (CSP) and cloud service partners (CSN) as they need a SaaS application environment to meet their demands on security. The requirements are general and independent of any service or scenario specific model (e.g. web services, or representational state transfer (REST)), assumptions or solutions.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_