Geneva, 7 January 2011

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

|  |  |  |
| --- | --- | --- |
| Ref:Tel:Fax: | **TSB Circular 158**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 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.1261, X.1500, X.1520, and X.1521 in accordance with the provisions of Resolution 1, Section 9, of WTSA (Johannesburg, 2008), Geneva, 20 April 2011** |

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 11 to 20 April 2011, intends to apply the procedure described in Resolution 1, Section 9, of WTSA (Johannesburg, 2008) for the approval of the above-mentioned draft new Recommendations.

2 The titles, summaries and location of the draft new ITU-T Recommendations proposed for approval will be found in **Annex 1**.

3 Any ITU Member State, Sector Member or Associate 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 30 March 2011** whether your Administration assigns authority to Study Group 17 that these draft new 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 new Recommendations.

5 If 70% or more of the replies from Member States support consideration for approval of these draft new Recommendations at the Study Group meeting, one Plenary session will be devoted **on 20 April 2011** 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 5/17.

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,

Malcolm Johnson
Director of the Telecommunication
Standardization Bureau

**Annex: 1**

ANNEX 1
(to TSB Circular 158)

**Summary and location of the texts**

**Draft new Recommendation ITU-T X.1500 (X.cybex), Cybersecurity information exchange techniques
COM 17 – R 25** *(shortly available on the web)*

**Summary**

This Recommendation describes techniques for exchanging cybersecurity information. These techniques can be used individually or in combinations, as desired or appropriate, to enhance cybersecurity through coherent, comprehensive, global, timely and assured information exchange. No obligations to exchange information are implied, nor are the means of acquisition or ultimate use of the information treated.

**Draft new Recommendation ITU-T X.1520 (X.cve), Common vulnerabilities and exposure (CVE)
COM 17 – R 26**

**Summary**

This Recommendation addresses a structured means to exchange common information security vulnerabilities and exposures (CVE) that aims to provide common names for publicly known problems in the commercial or open source software used in communications networks, end user devices, or any of the other types of information and communication technology (ICT) capable of running software. The goal of this Recommendation is to make it easier to share data across separate vulnerability capabilities (tools, repositories, and services) with this common naming. This Recommendation is designed to allow vulnerability databases and other capabilities to be linked together, and to facilitate the comparison of security tools and services. As such, this Recommendation does not contain information such as risk, impact, fix information, or detailed technical information. This Recommendation only contains the standard identifier number with status indicator, a brief description, and references to related vulnerability reports and advisories.

The intention of this Recommendation is to be comprehensive with respect to all publicly known vulnerabilities and exposures. While this Recommendation is designed to contain mature information, the primary focus is on identifying vulnerabilities and exposures that are detected by security tools and any new problems that become public, and then addressing any older security problems that require validation.

**Draft new Recommendation ITU-T X.1521 (X.cvss), Common vulnerability scoring system (CVSS)
COM 17 – R 27** *(shortly available on the web)*

**Summary**

This Recommendation provides an open framework for communicating the characteristics and impacts of information and communication technology (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. This Recommendation covers common vulnerability scoring system (CVSS), where the goal 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.1261 (X.EVcert), Extended validation certificate framework (EVcert)
COM 17 – R 30**

Summary

This Recommendation covers the extended validation certificate framework and is an integrated combination of technologies, protocols, identity proofing, lifecycle management, and auditing practices that describe the minimum requirements that must be met in order to issue and maintain extended validation certificates (“EV Certificates”) concerning an organization. Subject organization information from valid “EV Certificates” can then be displayed in a special manner by certain relying-party software applications (e.g., browser software) in order to provide users with a trustworthy confirmation of the identity of the entity that controls the website or other services they are accessing. Although initially intended for use in establishing web-based data communication conduits via transport layer security - or secure socket layer security (TLS/SSL) protocols, extensions are envisioned for secure / multipurpose Internet mail extensions (S/MIME), time-stamping, voice-over-Internet protocol (VoIP), instant messaging (IM), web services, etc.

The primary purposes of this Recommendation are to: 1) identify the legal entity that controls a web or service site, and 2) enable encrypted communications with that site. The secondary purposes include significantly enhancing cybersecurity by helping establish the legitimacy of an organization claiming to operate a website, and providing a vehicle that can be used to assist in addressing problems related to distributing malware, phishing, identity theft, and diverse forms of online fraud.

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