Geneva, 9 September 2011

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

|  |  |  |
| --- | --- | --- |
| Ref:Tel:Fax: | **TSB Circular 228**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 Recommendations ITU-T X.1037, X.1500.1, X.1524 and X.1541 in accordance with the provisions of Resolution 1, Section 9, of WTSA (Johannesburg, 2008), Geneva, 2 March 2012** |

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 20 February to 2 March 2012, 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, 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 8 February 2012** 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 2 March 2012** 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,

Malcolm Johnson
Director of the Telecommunication
Standardization Bureau

**Annex: 1**

ANNEX 1
(to TSB Circular 228)

**Summary and location of the texts**

**Draft new Recommendation ITU-T X.1037 (X.rev), Architectural systems for security controls for preventing fraudulent activities in public carrier networks
COM 17 – R 41**

**Summary**

Recommendation ITU-T X.1037 describes a methodology for evaluation systems of security controls for preventing fraudulent activities, and criteria for selection of these systems, with regard to architectural characteristics of communications service provider (CSP) networks at their present-day level of development. The Recommendation includes technical methods for addressing security controls and estimating losses caused by fraudulent activities, and also provides guidelines for the exchange of information related to fraudulent activities.

**Draft Recommendation ITU-T X.1500.1 (X.cybex.1), Procedures for the registration of arcs under the object identifier (OID) arc for cybersecurity information exchange
COM 17 – R 42**

**Summary**

This Recommendation provides for the registration of OID arcs which enable coherent, unique and global identification of cybersecurity information as well as of organizations exchanging that information and associated policies. This Recommendation specifies the information and justification to be provided when requesting an OID for cybersecurity information exchange purposes, and the procedures for the operation of the Registration Authority.

**Draft Recommendation ITU-T X.1524 (X.cwe), Common weakness enumeration (CWE)
COM 17 – R 43**

**Summary**

This Recommendation on the use of the common weakness enumeration (CWE) provides a structured means to exchange information security weaknesses that provides 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 communications technology (ICT) capable of running software. The goal of CWE is to enable more effective discussion, description, selection, and use of software security tools and services that can find these weaknesses in source code and operational systems as well as better understanding and management of software weaknesses related to architecture and design. This Recommendation defines the use of CWE to provide a mechanism for software security tools, services, knowledge bases and other capabilities to be used together, and to facilitate the comparison of security tools and services. CWE also offers supportive context information about possible risks, impacts, fix information, and detailed technical information about what the software weaknesses could mean to a software system. The repository of CWE Identifiers and the associated context information is available at [cwe.mitre.org/data] as XML or pdf. A web accessible version of the same content is available at [http://cwe.mitre.org/data/slices/2000.html]

The intention of CWE, the use of which is defined in this Recommendation, is to be comprehensive with respect to the software architecture, design, coding, and deployment errors that are the root causes of vulnerabilities and exposures. While CWE is designed to contain mature information, the primary focus is on identifying, educating, and describing these root causes of vulnerabilities and exposures so they can be avoided by developers, tested for, and managed by development teams as well as consistently reported by security tools and services.

**Draft Recommendation ITU-T X.1541 (X.iodef), Incident object description exchange format
COM 17 – R 44**

Summary

The incident object description exchange format (IODEF) defines a data representation that provides a framework for sharing information commonly exchanged by Computer Security Incident Response Teams (CSIRTs) about computer security incidents. This Recommendation describes the information model for the IODEF and provides an associated data model specified with XML Schema.

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