Geneva, 8 March 2012

|  |  |
| --- | --- |
| **Telecommunication Standardization Bureau** |  |
|  |  |

|  |  |  |
| --- | --- | --- |
| Ref:  Tel:  Fax: | **TSB Circular 269**  COM 17/MEU  +41 22 730 5866 +41 22 730 5853 | - To Administrations of Member States of the Union |
| E-mail: | [tsbsg17@itu.int](mailto: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.1054, X.1254, X.1527, X.1528, X.1528.1, X.1528.2, X.1528.3, X.1528.4, X.1541, X.1580, and X.1581 in accordance with the provisions of Resolution 1, Section 9, of WTSA (Johannesburg, 2008), Geneva, 7 September 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 29 August to 7 September 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 16 August 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 7 September 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 269)**

**Summary and location of the texts**

**Draft new Recommendation ITU-T X.1054 (X.isgf), Information technology - Security techniques - Governance of information security  
COM 17 – R 49**

**Summary**

This Recommendation | International Standard provides guidance on the governance of information security.

Information security has become a key issue for organisations. Not only are there increasing regulatory requirements but also the failure of an organisation’s information security measures can have a direct impact on an organisation’s reputation.

Therefore, the governing body, as part of its governance responsibilities, is increasingly required to oversee information security to ensure the objectives of the organisation are achieved.

In addition, governance of information security provides a powerful link between an organisation’s governing body, executive management and those responsible for implementing and operating an information security management system.

It provides the mandate essential for driving information security initiatives throughout the organisation.

Furthermore, an effective governance of information security ensures that the governing body receives relevant reporting - framed in a business context - about information security-related activities. This enables pertinent and timely decisions about information security issues in support of the strategic objectives of the organisation.

**Draft new Recommendation ITU-T X.1254 (X.eaa) | ISO/IEC 29115, Information technology — Security techniques — Entity authentication assurance framework  
COM 17 – R 61**

**Summary**

This Recommendation | International Standard defines four levels of entity authentication assurance (i.e., LoA 1 – LoA 4); and the criteria and threats for each of the four levels of entity authentication assurance. Additionally it:

* specifies a framework for managing the assurance levels;
* based on a risk assessment, provides guidance concerning control technologies that to be used to mitigate authentication threats to authentication;
* provides guidance for mapping the four levels of assurance to other authentication assurance schemas; and
* provides guidance for exchanging the results of authentication that are based on the four levels of assurance.

**Draft new Recommendation ITU-T X.1527 (X.xccdf), Extensible configuration checklist description format  
COM 17 – R 50**

**Summary**

This Recommendation specifies the data model and Extensible Markup Language (XML) representation for the Extensible Configuration Checklist Description Format (XCCDF). An XCCDF document is a structured collection of security configuration rules for some set of target systems. The XCCDF specification is designed to support information interchange, document generation, organizational and situational tailoring, automated compliance testing, and scoring. The specification also defines a data model and format for storing results of security guidance or checklist testing. The intent of XCCDF is to provide a uniform foundation for expression of security checklists and other configuration guidance, and thereby foster more widespread application of good security practices. This is achieved by listing the relevant clauses of NIST Interagency Report 7275 Revision 4, Specification for the Extensible Configuration Checklist Description Format (XCCDF) Version 1.2, and showing whether they are normative or informative.

**Draft new Recommendation ITU-T X.1528 (X.cpe), Common platform enumeration  
COM 17 – R 51**

**Summary**

This Recommendation on common platform enumeration (CPE) provides a structured method of describing and identifying classes of applications, operating systems, and hardware devices present among an enterprise's computing assets. CPE is defined through a set of specifications in a stack-based model, where capabilities are based on simpler, more narrowly defined elements that are specified lower in the stack. The stack consists of a Dictionary specification and an Applicability Language specification that rely on a Name Matching specification which relies on a Naming specification.

**Draft new Recommendation ITU-T X.1528.1 (X.cpe.1), Common platform enumeration naming  
COM 17 – R 52**

Summary

This Recommendation on common platform enumeration (CPE) naming defines the logical structure of names for IT product classes and the procedures for binding and unbinding these names to and from machine-readable encodings. This Recommendation also defines and explains the requirements that IT products must meet to claim conformance with this Recommendation. This is achieved by listing the relevant clauses of the NIST Interagency Report 7696 Common Platform Enumeration: Name Matching Specification version 2.3 and showing whether they are normative or informative.

**Draft new Recommendation ITU-T X.1528.2 (X.cpe.2), Common platform enumeration name matching  
COM 17 – R 53**

Summary

This Recommendation defines the specification for common platform enumeration (CPE) name matching. The CPE name matching specification is part of a stack of CPE specifications that support a variety of use cases relating to IT product description and naming. The CPE Name Matching specification provides a method for conducting a one-to-one comparison of a source CPE name to a target CPE name. In addition to defining the specification, this Recommendation also defines and explains the requirements that IT products must meet to claim compliance. This is achieved by listing the relevant clauses of the NIST Interagency Report 7696 Common Platform Enumeration: Name Matching Specification version 2.3 and showing whether they are normative or informative.

**Draft new Recommendation ITU-T X.1528.3 (X.cpe.3), Common platform enumeration dictionary  
COM 17 – R 54**

Summary

This Recommendation defines the common platform enumeration (CPE) dictionary specification. The CPE dictionary specification is a part of a stack of CPE specifications that support a variety of use cases relating to information technology (IT) product description and naming. An individual CPE dictionary is a repository of IT product names, with each name in the repository identifying a unique class of IT product in the world. This specification defines the semantics of the CPE Dictionary data model and the rules associated with CPE dictionary creation and management. This Recommendation also defines and explains the requirements that IT products and services, including CPE dictionaries, must meet to claim compliance with this Recommendation. This is achieved by listing the relevant clauses of the NIST Interagency Report 7697 Common Platform Enumeration: Name Matching Specification version 2.3 and showing whether they are normative or informative.

**Draft new Recommendation ITU-T X.1528.4 (X.cpe.4), Common platform enumeration applicability language  
COM 17 – R 55**

Summary

This Recommendation defines the specification for common platform enumeration (CPE) applicability language. The CPE applicability language specification is part of a stack of CPE specifications that support a variety of use cases relating to IT product description and naming. The CPE applicability language data model builds on top of other CPE specifications to provide the functionality required to allow CPE users to construct complex groupings of CPE names to describe IT platforms. These groupings are referred to as applicability statements because they are used to designate the platforms to which particular guidance, policies, etc. apply. This Recommendation defines the semantics of the CPE applicability language data model and the requirements that IT products and CPE applicability language documents must meet to claim compliance with this Recommendation.

This is achieved by listing the relevant clauses of the NIST Interagency Report 7698: Common Platform Enumeration Applicability Language Specification version 2.3 and showing whether they are normative or informative.

**Draft new Recommendation ITU-T X.1541 (X.iodef), Incident object description exchange format  
COM 17 – R 56**

Summary

This Recommendation describes the information model for the incident object description exchange format (IODEF) and provides an associated data model specified with XML Schema. The IODEF specifies a data model representation for sharing information commonly exchanged by Computer Security Incident Response Teams (CSIRTs) and service providers (SPs) about computer security or other incident types. This is achieved by listing the relevant clauses of RFC 5070 and showing whether they are normative or informative.

**Draft new Recommendation ITU-T X.1580 (X.rid), Real-time inter-network defense  
COM 17 – R 57**

Summary

This Recommendation on real-time inter-network defense (RID) outlines a proactive inter-network communication method to facilitate the automation of sharing incident handling information. Implementations may integrate with existing incident management systems as well as detection, source identification, and mitigation mechanisms for a more complete incident handling solution. RID specifies a method to securely communicate incident information, enabling the exchange of incident object description exchange format (IODEF) extensible markup language (XML) documents. RID provides a technical means to convey security, policy, and privacy controls to enable the exchange of potentially sensitive information. The technical capabilities can be mapped to the appropriate policies to enable service providers or organizations the option to make appropriate decisions according to their policies.

This Recommendation specifies RID by listing the relevant clauses of RFC 6545 and showing whether they are normative or informative.

**Draft new Recommendation ITU-T X.1581 (X.ridt), Transport of real-time inter-network defense messages  
COM 17 – R 58**

Summary

This Recommendation specifies a transport protocol for real-time inter-network defense (RID) based upon the passing of RID messages over hypertext transfer protocol/transport layer security (HTTP/TLS). This is achieved by listing the relevant clauses of RFC 6546 and showing whether they are normative or informative.

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