|  |  |
| --- | --- |
| **电信标准化局** | **logo_C_** |
|  |  |

 2011年4月28日，日内瓦

|  |  |  |
| --- | --- | --- |
| 文号：电话：传真： | **电信标准化局第190号通函**COM 17/MEU+41 22 730 5866+41 22 730 5853 | - 致国际电联各成员国主管部门 |
| 电子邮件： | tsbsg17@itu.int | **抄送：**- ITU-T部门成员；- ITU-T部门准成员；- ITU-T学术成员；- 第17研究组正副主席；- 电信发展局主任；- 无线电通信局主任 |

|  |  |
| --- | --- |
| 事由： | **第17研究组按照世界电信标准化全会（2008年，约翰内斯堡）第1号决议第9节的规定为批准新的ITU-T X.1211、X.1246、X.1253和X.1570建议书草案而召开的会议****2011年9月2日，日内瓦** |

尊敬的先生/女士：

1 应第17研究组（安全）主席的请求，我荣幸地告知您，该研究组将于2011年8月24日至9月2日召开会议，并将采用世界电信标准化全会（2008年，约翰内斯堡）第1号决议第9节规定的程序来批准上述新的建议书草案。

2 建议批准的经修订的ITU-T建议书草案[和新的ITU-T建议书草案]的摘要及其出处见**附件1**。

3 所有了解自己或他人持有的专利可能整体或部分地涉及建议批准的（一项或多项）建议书草案内容的国际电联成员国、部门成员、部门准成员或学术机构，均需按照 ITU-T/ITU-R/ISO（国际标准化组织）/IEC（国际电工委员会）的共同专利政策，向电信标准化局披露这类信息。

可通过ITU-T网站（[www.itu.int/ITU-T/ipr/](http://www.itu.int/itu-t/ipr/)）在网上获取已公布的专利信息。

4 考虑到第1号决议第9节的规定，请您在**2011年8月11日**协调世界时24时之前告知我，贵主管部门是否同意授权第17研究组在该研究组会议上审议并批准上述修订建议书草案或新建议书草案。

如有成员国认为不应进入审议批准程序，应阐明其反对原因并提出可能的修改意见，以推动对相关修订建议书草案或新建议书草案的进一步审议，以便批准。

5 如果70％以上的成员国在回复中支持在该研究组会议上审议并批准上述修订建议书草案或新建议书草案，则将于**2011年9月2日**召开一次全体会议，实施该批准程序。

为此，我邀请贵主管部门派出一名代表参加会议。请**国际电联成员国的主管部门**提供其代表团团长的姓名。如果贵主管部门希望由一家经认可的运营机构、一个科学或工业组织或处理电信问题的另一实体作为代表参加会议，则应按照国际电联《公约》第19条第239款的规定，将有关情况适时向主任通报。

6 有关第17研究组会议的议程和所有相关信息将在第6/17号集体函中提供。

7 会后电信标准化局主任将以通函的形式通报就这几份建议书做出的决定。此信息还将在《国际电联操作公报》中公布。

顺致敬意!

电信标准化局主任
 马尔科姆•琼森

**附件：1件**

附件 1
（附于电信标准化局190号通函）

**案文摘要和出处**

**新的ITU-T X.1211（X.tb-ucc）建议书草案，网络追踪的可用性
COM 17 – R 33**

**摘要**

此建议书全面介绍了对单一或更为复杂的群体业务提供商当中出现的某些网络问题采取响应措施的跟踪工作。跟踪有助于发现入侵点、路径、部分路径或问题网络事件的来源。这一信息有助于业务提供商缓解这类事件的影响。

**新的ITU-T X.1246 （X.tcs-2）建议书草案，打击VoIP垃圾信息的基于实时屏蔽列表（RBL）的框架
COM 17 – R 34**

**摘要**

此建议书提供了一个打击VoIP垃圾信息的基于RBL的技术框架，其中包括四个功能实体：VoIP垃圾信息防御系统（VSPS）、VoIP垃圾信息防御策略服务器（VSPPS）、用于防范VoIP垃圾信息的RBL中央系统（VSP-RBL）和用户声望系统（URS）。此建议书还具体介绍了每个反VoIP垃圾信息功能实体的功能、程序和接口。

**新的ITU-T X.1253（X.idmsg）建议书草案，身份管理系统安全导则
COM 17 – R 38**

**摘要**

本建议书为身份管理（IdM）系统提供了安全导则。该导则规定了为向下一代网络（NGN）或网络空间环境提供安全身份服务而部署和操作IdM系统的方法，重点提供官方有关如何利用这种安全机制保护通用IdM系统的意见，还提供了两个IdM系统互操作时所需的适用安全程序。

**新的ITU-T X.1570（X.cybex-disc）建议书草案，网络安全信息交换中的发现机制
COM 17 – R 35**

摘要

本建议书提供了网络信息发现框架和将它付诸实施的机制。发现可被视为网络安全信息周期中的一个阶段，紧邻信息的发布和获取这些信息发现中完整和必要的阶段。因此这一框架涉及公布网络安全信息、获取候选列表并取得必要信息的方法。只要发现机制符合框架要求，它可与任意机制一起实施，而这些机制当中包括也在本建议书中得到阐述的基于目标标识符（OID）和基于资源描述框架（RDF）的发现程序。

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