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

 2011年1月7日，日内瓦

|  |  |  |
| --- | --- | --- |
| 文号：电话：传真： | **电信标准化局第158号通函**COM17/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；- 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ITU-T X.1261、X.1500、X.1520和X.1521新建议书草案而召开的会议****2011年4月20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4月11至20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建议书草案。

2 建议批准的新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、部门成员或部门准成员，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3月30日**协调世界时24时前告知我，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4月20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行机构、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5/17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此（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
（电信标准化局158号通函）

**案文摘要和出处**

**ITU-T X.1500新建议书草案 (X.cybex)“网络安全信息的交换方法”
COM 17 – R 25号文件**（将很快在网上公布）

摘要

本建议书描述了交换网络安全信息的方法。这些方法可根据需要或酌情单独使用，也可组合使用，以便通过前后一致、综合、全面、及时和有保障地交换信息来改善网络安全。此举并不意味着有交换信息的义务，也不涉及所处理信息的获取方式或最终使用。

**ITU-T X.1520新建议书草案(X.cve)“通用漏洞和暴露”（CVE）
COM 17 – R 26号文件**

摘要

本建议书涉及一种交换通用信息安全漏洞和暴露（CVE）的结构性方法，该方法旨在提供在通信网络、最终用户设备或任何其他可运行软件的信息通信技术（ICT）中所使用的商业或开源软件中众所周知问题的通用名称。本建议书的目标是借助该通用命名，更加容易地在不同的漏洞能力（工具、存储库、服务）之间分享数据。本建议书旨在允许漏洞数据库和其他能力可连结在一起并有助于安全工具和服务的比较。如此，本建议书并不包含风险、影响、调整信息或详细技术信息等信息。本建议书只包含标准标识符号码以及状态指示符、简要描述以及对相关漏洞报告和公告的参引。

本建议书的目的是在所有众所周知的漏洞和暴露方面做到详尽、全面。尽管此建议书有意包含成熟可靠的信息，但其主要重点还是确定由安全工具发现的漏洞和暴露以及为公众所知的任何新问题，并随后解决需要验证的任何陈旧安全问题。

**ITU-T X.1521新建议书草案(X.cvss)“通用漏洞评估系统”（CVSS）
COM 17 – R 27号文件**（将很快在网上公布）

摘要

本建议书提供了在通信网络、最终用户设备或任何其他可运行软件的信息通信技术（ICT）中交流漏洞特性和影响的开放性框架。本建议书涵盖了通用漏洞评估系统（CVSS），其目标是使ICT管理人员、漏洞公告人员、安全服务销售商、应用销售商和研究人员在评估ICT漏洞时采用统一的措辞。

**ITU-T X.1261 (X.EVcert) 新建议书草案“扩展验证证书框架”（EVcert）
COM 17 – R 30号文件**

摘要

本建议书涵盖了扩展验证证书框架且是技术、协议、身份证明、周期管理和审核实践等描述必须满足的最低要求，以便发放和持有涉及一个组织扩展验证证书（EV Certificate）的整体组合。随后，有效“扩展验证证书”的管理信息可通过某些可信赖方软件应用（如浏览器软件等）以特别的方式显示，以便向用户提供控制网站的实体身份或其正在获取的其他服务的可靠确认。尽管起初是计划用于通过传输层保密或安全套接层保密（TLS/SSL）协议来建立网页数据交流渠道，但扩展被设想用于安全多功能互联网邮件扩展（S/MIME）、时戳、网络电话、即时通信、网络服务等。

本建议书的主要目标有：1) 确定控制网站或服务站点的法律实体，以及2) 实现与该站点的加密通信。第二个目标包含通过帮助确立宣称运营某个网站的一个组织的合法性并提供可用来协助解决与传播恶意软件、身份盗窃和各种在线诈骗等有关问题的载体，来显著改善网络安全。

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