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

2014年5月8日，日内瓦

|  |  |  |
| --- | --- | --- |
| 文号: | **电信标准化局第101号通函**  TSB Workshops/ME |  |
| 联系人： | Martin Euchner |  |
| 电话： 传真：  电子 邮件： | +41 22 730 5866 +41 22 730 5853  [tsbworkshops@itu.int](mailto:tsbworkshops@itu.int) | - 致国际电联各成员国主管部门；  - 致ITU-T部门成员；  - 致ITU-T部门准成员；  - 致ITU-T学术成员  **抄送：**  - ITU-T研究组正副主席；  - 电信发展局主任；  - 无线电通信局主任 |

|  |  |
| --- | --- |
| 事由： | **国际电联关于“ICT安全标准化工作对于发展中国家的挑战”讲习班– 2014年9月15-16日，日内瓦** |

尊敬的先生/女士，

1 我谨通知您，为期一天半的“**ICT安全标准化工作对于发展中国家的挑战**”讲习班将于2014年9月15日下午至16日在瑞士日内瓦国际电联总部举办。该讲习班之后，将于2014年9月17日至26日在同一地点举办ITU-T第17研究组会议。

讲习班将于第一天的14:00开始。与会者的注册工作将自13:00开始。有关会议厅的详尽信息将在国际电联总部各入口处的屏幕上显示。

2 讨论将仅用英文进行。

3 国际电联成员国、部门成员和部门准成员、学术机构以及愿参加此工作的来自国际电联成员国的任何个人均可参加此讲习班。这里所指的“个人”亦包括作为国际、区域和国家组织成员的个人。讲习班不收取任何费用，但亦不发放与会补贴。但将向随后召开的ITU-T第17研究组会议提供与会补贴，其中将涵盖本次国际电联安全讲习班。

4 此次讲习班的主要目的是在ITU-T第17研究组活动的基础上，介绍并讨论ICT安全方面的挑战，特别是对于发展中国家的挑战。本次国际电联安全讲习班侧重于标准化领域，旨在向发展中国家提供有关国际ICT安全标准方面的具体建议和最佳做法， 从而提高发展中国家标准化工作的能力。讲习班还旨在完善和提高与国际电联电信发展部门和其他标准制定组织之间的协作。

讲习班将汇聚这一领域的知名专家，他们分别来自发展中国家、国际电联成员国、监管机构、政策制定机构和私营部门（服务供应商、电信运营商、制造商和解决方案提供商）、学术界、标准化组织、论坛和行业联盟。

5 讲习班的日程草案载于**附件1**。日程草案也将通过ITU-T活动网站[www.itu.int/en/ITU-T/Workshops-and-Seminars/ict-sec-chaldc/](http://www.itu.int/en/ITU-T/Workshops-and-Seminars/ict-sec-chaldc/)提供，并将随着获得新的或修订信息进行定期更新。

6 国际电联的主要会议厅和日内瓦国际会议中心（CICG）内均设有无线局域网设施，供代表使用。详细信息见ITU-T网站（<http://www.itu.int/ITU-T/edh/faqs-support.html>）。

7 **附件2**中有一份酒店确认单（酒店清单见<http://www.itu.int/travel/>），供参考。关于酒店住宿、交通和签证的要求 可在ITU-T网站找到：[www.itu.int/en/ITU-T/Workshops-and-Seminars/ict-sec-chaldc/](http://www.itu.int/en/ITU-T/Workshops-and-Seminars/ict-sec-chaldc/)

8 为便于电信标准化局就该讲习班的组织做出必要安排，我希望您能通过网址[www.itu.int/en/ITU-T/Workshops-and-Seminars/ict-sec-chaldc/](http://www.itu.int/en/ITU-T/Workshops-and-Seminars/ict-sec-chaldc/)以在线形式向电信标准化局尽早、但**不迟于2014年9月1日**进行注册。**请注意，讲习班与会者的预注册仅以在线方式进行**。

9 我们谨在此提醒您，一些国家的公民需要获得签证才能入境瑞士并在此逗留。**签证必须至少在会议召开日的六（6）个星期前向驻贵国的瑞士代表机构（使馆或领事馆）申请，并随后领取**。如贵国没有此类机构，则请向驻离贵国最近的国家的此类机构申请并领取。

如果**国际电联成员国、部门成员、部门准成员或学术机构**遇到了问题，国际电联可根据他们向电信标准化局提出的正式请求与相关瑞士当局接触，以便为发放签证提供方便，但仅限于在所述的六个星期内办理。此类请求应通过您所代表的主管部门或实体发出的正式信函提出。该函必须说明申请签证人员的姓名和职务、出生日期、护照号码以及护照签发日期和失效日期，并需附有一份经ITU-T所述讲习班批准的注册确认通知，而且必须通过传真（传真号码：+41 22 730 5853）或电子邮件（[tsbreg@itu.int](mailto:tsbreg@itu.int)）发至电信标准化局，上面注明“**visa request**”（“**签证申请**”）。**另请注意，国际电联仅能向国际电联成员国、国际电联部门成员、国际电联部门准成员和学术机构的代表提供帮助。**

顺致敬意！

电信标准化局主任

马尔科姆•琼森

**附件：2件**

ANNEX 1

(To TSB Circular 101)

**Draft workshop programme**

|  |  |
| --- | --- |
| **Day 1: 15 September 2014** | |
| **Time** | **Sessions** |
| 14:00 – 14:30 | Welcome and Opening Remarks  The objective of the workshop is to present activities and achievements of standardization on cybersecurity, data protection, trust services and cloud computing, focus in methodology of securing ICT within critical infrastructure, hear a reaction from security industry, address the interests and needs of users, and encourage collaboration between SDOs in security standardization for the special needs of developing countries. |
| 14:30 – 16:30 | Session 1 – ICT infrastructure development, new security threats and counter-measures  Today the critical role of ICT in virtually all socio-economic activities cannot be over-emphasised. Disruption of the ICT infrastructure can therefore result in disastrous consequences for governments as well as citizens’ social wellbeing. The need to ensure ICT robustness against cyber attacks remains a key challenge at national as well as global level.  This session will address the current situation of ICT infrastructure development and the challenges such as new security threats and countermeasures including new trends in ICT. The session will highlight best practices in formulation of national strategies, government and industrial collaboration, sound legal formulation to fight cybercrime, national incident capabilities, and importance of rising national awareness on cybersecurity, among other things. |
| 16:30 – 16:45 | Coffee Break |
| 16:45 – 18:30 | Session 2 – End user security round table from both public and private sectors  After a set of presentations that highlight “end user security” in terms of identified security issues and requirements from each presenter’s perspective, a roundtable discussion will explore and identify security requirements/security capabilities required from the end user’s view points and how to utilize security technologies/standards.  Members of the roundtable discussion will cover both public and private sectors such as critical information infrastructure sectors, medical sector, educational sector (university) and telecom/mobile sectors etc. |

|  |  |
| --- | --- |
| **Day 2: 16 September 2014** | |
| **Time** | **Sessions** |
| 09:00 – 10:45 | Session 3 – Cybersecurity and data protection  Widespread use of internet technologies and increasing number of cyber threats make cyber security more important. In this session, representatives from Congo and Kenya will share their cyber security experiences and challenges. Also, cyber security standards and information exchange techniques will be focused by the experts. |
| 10:45 – 11:00 | Coffee Break |
| 11:00 – 12:45 | Session 4 – ICT role in critical infrastructure protection  Critical infrastructure is a term used by governments to describe assets that are essential for the functioning of a society, such as energy, transportation, telecommunication, water supply, agriculture, public health, financial services, etc. Most critical infrastructures rely on Information and Communication Technologies (ICTs), including industrial control systems (ICS), to perform essential functions. This dependency represents potential vulnerabilities and risks to operations. This section will focus on existing ICT security standards, guidelines, methodologies, and practices to enable critical infrastructure providers to achieve the resilience required. |
| 12:45 – 14:00 | Lunch Break |
| 14:00 – 15:45 | Session 5 – Trust services and cloud security  Cloud computing is a model for enabling service user’s ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources. Identity management (IdM) is the management of the life cycle and use of identity information. This session will focus on presenting existing ICT security standards, guidelines, and best practices in the area of cloud computing security and identity management to ensure trust services and cloud computing security. |
| 15:45 – 16:00 | Coffee Break |
| 16:00 – 17:45 | Session 6 – Security standardization challenges  After a set of presentations that highlight ICT security standardization efforts in international and regional bodies, a roundtable discussion will explore security standardization challenges. Topics will include insights on the benefits and challenges associated with collaboration and cooperation and on challenges associated with ensuring standards will meet the needs of users, especially those in developing countries. |
| 17:45 – 18:30 | Closing panel – Workshop Summary and Closing Remarks |
| 18:30 – 20:00 | Reception and social networking event |

ANNEX 2  
 (to TSB Circular 101)

|  |
| --- |
| *This confirmation form should* ***be sent direct to the hotel*** *of your choice* |

|  |  |  |
| --- | --- | --- |
|  | **INTERNATIONAL TELECOMMUNICATION UNION** |  |

**TELECOMMUNICATION STANDARDIZATION SECTOR**

*ITU Workshop on* ***“ICT Security Standardization Challenges for Developing Countries”****from 15 to 16 September 2014 in Geneva*

*Confirmation of the reservation made on (date) -------------------------- with (hotel) --------------------------------*

***at the ITU preferential tariff***

*------------ single/double room(s)*

*arriving on (date)----------------------------- at (time) ------------- departing on (date)--------------------------------*

***GENEVA TRANSPORT CARD:*** *Hotels and residences in the canton of Geneva now provide a free "Geneva Transport Card" valid for the duration of the stay. This card will give you free access to Geneva public transport, including buses, trams, boats and trains as far as Versoix and the airport.*

*Family name* -------------------------------------------------------------------------------------------------------------------

*First name*  ------------------------------------------------------------------------------------------------------------------

*Address*  ------------------------------------------------------------------------ *Tel: -------------------------------*

*----------------------------------------------------------------------------------------- Fax: -------------------------------*

*----------------------------------------------------------------------------------------- E-mail:* ------------------------------

*Credit card to guarantee this reservation*: AX/VISA/DINERS/EC (*or* *other) -----------------------------------*

*No.* -------------------------------------------------------- *valid until* ------------------------------------------------

*Date* ------------------------------------------------------ *Signature*  ---------------------------------------------------