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

Geneva, 8 May 2014

|  |  |  |
| --- | --- | --- |
| Ref:  Contact:  Tel:  Fax: | **TSB Circular 101**  TSB Workshops/ME  Martin Euchner  +41 22 730 5866 +41 22 730 5853 | - To Administrations of Member States of the Union;  - To ITU-T Sector Members;  - To ITU-T Associates;  - To ITU-T Academia |
| E-mail: | [tsbworkshops@itu.int](mailto:tsbworkshops@itu.int) | **Copy:**  - To the Chairman and Vice-Chairmen of ITU-T Study Groups;  - To the Director of the Telecommunication Development Bureau;  - To the Director of the Radiocommunication Bureau |

|  |  |
| --- | --- |
| Subject: | **ITU Workshop on ICT Security Standardization Challenges for Developing Countries - Geneva, Switzerland, 15 – 16 September 2014** |

Dear Sir/Madam,

1 I am pleased to inform you that a one-and-half day workshop on "**ICT Security Standardization Challenges for Developing Countries**" will take place at ITU headquarters in Geneva, Switzerland from 15 (p.m.) to 16 September 2014. This workshop will be followed by the fourth ITU-T Study Group 17 meeting from 17 to 26 September 2014 at the same venue.

The workshop will open at 1400 hours on the first day. Registration will begin at 1300 hours. Detailed information concerning the meeting room will be displayed on screens at the entrances to ITU headquarters.

2 Discussions will be held in English only.

3 Participation is open to ITU Member States, Sector Members, Associates, Academic Institutions and to any individual from a country which is a member of ITU who wishes to contribute to the work. This includes individuals who are also members of international, regional and national organizations. The workshop is free of charge and no fellowships will be granted. However, fellowships will be offered for the subsequent SG17 meeting to cover also this ITU security workshop.

4 The main objective of the workshop is to present and discuss ICT security challenges, in particular for Developing Countries on the basis of activities of ITU-T SG17. A focus of this ITU security workshop is the standardization domain, where the objective is to provide concrete advice and best practices of international ICT security standards to developing countries such that standardization competence of developing countries can be enhanced. The workshop also aims to improve and yield better collaboration with the ITU-D Sector and other standards-setting organizations.

The workshop will bring together leading specialists in the field, from Developing countries, ITU Member States, regulatory agencies, policy makers, private sector (service providers, telecommunication operators, manufacturers and solution providers), academia, standardization organizations, forums and consortia.

5 A draft workshop program is set out in **Annex 1.** It is also made available on the ITU event website: [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/). This website will be updated as new or modified information become available.

6 Wireless LAN facilities are available for use by delegates in the ITU main conference room areas and in the CICG (Geneva International Conference Centre) building. Detailed information is available on the ITU-T website (<http://www.itu.int/ITU-T/edh/faqs-support.html>).

7 For your convenience, a hotel confirmation form is enclosed as **Annex 2** (see <http://www.itu.int/travel/> for the list of hotels). Detailed information on hotel accommodation, transportation and visa requirements can be found on the ITU-T website: [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 To enable TSB to make the necessary arrangements concerning the organization of the workshop, I should be grateful if you would register via the on-line form at [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/) as soon as possible, **but not later than 1 September 2014**. **Please note that pre-registration of participants to workshops is carried out exclusively *online***.

9 I would remind you that citizens of some countries are required to obtain a visa in order to enter and spend any time in Switzerland. **The visa must be requested at least six (6) weeks before the date of beginning of the workshop** and obtained from the office (embassy or consulate) representing Switzerland in your country or, if there is no such office in your country, from the one that is closest to the country of departure.

If problems are encountered by **ITU Member States, Sector Members, Associates or Academic Institutions**, and at the official request made by them to TSB, the Union can approach the competent Swiss authorities in order to facilitate delivery of the visa but only within the period mentioned of six weeks. Any such request should be made by official letter from the administration or entity you represent. This letter must specify the name and functions, date of birth, number, dates of issue and expiry of passport of the individual(s) for whom the visa(s) is/are requested and be accompanied by a copy of the notification of confirmation of registration approved for the ITU-T workshop in question, and must be sent to TSB by fax (+41 22 730 5853) or e-mail ([tsbreg@itu.int](mailto:tsbreg@itu.int)), bearing the words **“visa request”**. **Please also note that ITU can assist only representatives of ITU Member States, ITU Sector Members, ITU Associates and ITU Academic Institutions.**

Yours faithfully,  
  
  
  
Malcolm Johnson  
Director of the Telecommunication  
Standardization Bureau  
  
 **Annexes: 2**

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*  ---------------------------------------------------