|  |  |
| --- | --- |
| **Oficina de Normalización de las Telecomunicaciones** |  |
|  |  |

Ginebra, 8 de mayo de 2014

|  |  |  |
| --- | --- | --- |
| Ref.:  Tel.: Fax: | **Circular TSB** **101**  TSB Workshops/ME  +41 22 730 5866 +41 22 730 5853 | - A las Administraciones de los Estados Miembros de la Unión;  - A los Miembros del Sector UIT-T;  - A los Asociados del UIT‑T;  - A las Instituciones Académicas del UIT-T |
| Correo-e: | [tsbworkshops@itu.int](mailto:tsbworkshops@itu.int) | **Copia**:  - A los Presidentes y Vicepresidentes de las Comisiones de Estudio del UIT-T;  - Al Director de la Oficina de Desarrollo de las Telecomunicaciones;  - Al Director de la Oficina de Radiocomunicaciones |

|  |  |
| --- | --- |
| Asunto: | **Taller del UIT-T sobre el tema "Dificultades en materia de normalización de la seguridad en las TIC para los países en desarrollo" – Ginebra (Suiza), 15-16 de septiembre de 2014** |

Muy Señora mía/Muy Señor mío:

1 Me complace informarle de que el taller sobre **"Dificultades en materia de normalización de la seguridad en las TIC para los países en desarrollo"**, de día y medio de duración, tendrá lugar en Ginebra, en la Sede de la UIT los días 15 (por la tarde) y 16 de septiembre de 2014, justo antes de la cuarta reunión de la Comisión de Estudio 17 del UIT-T, prevista del 17 al 26 de septiembre de 2014 también en la Sede.

El taller comenzará a las 14.00 horas del primer día. La inscripción comenzará a las 13.00 horas. En las pantallas situadas en las puertas de entrada de la Sede de la UIT se dará información detallada sobre las salas de reunión.

2 El taller se celebrará únicamente en inglés.

3 La participación está abierta a los Estados Miembros, a los Miembros de Sector, a los Asociados y a las Instituciones Académicas de la UIT, así como a cualquier persona de un país Miembro de la UIT interesada en contribuir a los trabajos. Quedan comprendidas las personas que también sean miembros de organizaciones nacionales, regionales e internacionales. La participación en el taller es gratuita pero ninguna beca será otorgada. No obstante, sí se ofrecen becas para la reunión ulterior de la CE 17, que abarcan también la participación en este taller de la UIT sobre seguridad.

4 El principal objetivo del taller es exponer y examinar las dificultades en materia de seguridad en las TIC, especialmente para países en desarrollo, sobre la base de las actividades de la CE 17 del UIT-T. Uno de los temas centrales de este taller de la UIT sobre seguridad es la normalización, a fin de proporcionar asesoramiento concreto y prácticas idóneas a los países en desarrollo acerca de normas internacionales de seguridad en las TIC y mejorar así sus competencias en materia de normalización. El taller tiene por objeto además mejorar y fomentar la colaboración con el UIT-D y otras organizaciones de normalización.

El taller reunirá a importantes especialistas en este campo, procedentes de países en desarrollo, Estados Miembros de la UIT, organismos reguladores, legisladores, sector privado (proveedores de servicio, operadores de telecomunicaciones, fabricantes y proveedores de soluciones), Instituciones Académicas, organizaciones de normalización, foros y consorcios.

5 En el **Anexo 1** se adjunta el proyecto de programa de trabajo del taller, que también puede consultarse en el sitio web del evento: [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/). Este sitio web se irá actualizando a medida que se vaya recibiendo información nueva o modificada.

6 Los delegados disponen de instalaciones de red de área local inalámbrica en las zonas aledañas a las principales salas de conferencias de la UIT y en el Centro Internacional de Conferencias de Ginebra (CICG). En el sitio web del UIT-T figura información más detallada (<http://www.itu.int/ITU-T/edh/faqs-support.html>).

7 A fin de facilitar sus trámites, se adjunta en el **Anexo 2** un formulario de confirmación de hotel (véase [http://www.itu.int/travel/](http://www.itu.int/travel) para la lista de hoteles). Puede encontrar información detallada sobre el alojamiento, el transporte y los requisitos de visado en el sitio web del UIT-T: [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 Para que la TSB pueda tomar las disposiciones necesarias sobre la organización del taller, le agradecería que se inscribiese a la mayor brevedad posible a través del formulario en línea disponible en [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/), y **a más tardar el 1 de septiembre de 2014**. **Le ruego que tome nota de que la preinscripción de los participantes en los talleres se lleva a cabo exclusivamente *en línea*.**

9 Le recordamos que los ciudadanos procedentes de ciertos países necesitan visado para entrar y permanecer en Suiza. **Ese visado debe solicitarse al menos seis (6) semanas antes de la fecha de inicio del taller** en la oficina (embajada o consulado) que representa a Suiza en su país o, en su defecto, en la más próxima a su país de partida.

Si **un Estado Miembro, un Miembro de Sector, un Asociado o una Institución Académica de la UIT** tropieza con problemas, y previa solicitud oficial de su parte a la TSB, la Unión puede intervenir ante las autoridades suizas competentes para facilitar la expedición de ese visado pero solamente durante el periodo mencionado de cuatro semanas. Toda solicitud al respecto debe enviarse por carta oficial de la administración o entidad que usted representa, en la cual se especificará el nombre y las funciones, la fecha de nacimiento y el número de pasaporte, con las fechas de expedición y expiración de las personas para las que se solicita el visado. La carta debe ir acompañada de una copia de la notificación de confirmación de inscripción aprobada para el taller de la UIT‑T correspondiente, y remitirse a la TSB con la indicación **"solicitud de visado"**, por fax (+41 22 730 5853) o correo electrónico ([tsbreg@itu.int](mailto:tsbreg@itu.int)). **Sírvase tomar nota de que la UIT puede ayudar únicamente a los representantes de los Estados Miembros, Miembros de Sector, Asociados e Instituciones Académicas de la UIT.**

Con este motivo, lo saluda atentamente.

Malcolm Johnson  
Director de la Oficina de Normalización  
de las Telecomunicaciones

**Anexos**: 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*  -------------------------------------------------

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