INTERNATIONAL TELECOMMUNICATION UNION

Telecommunication
Development Bureau

Place des Nations
CH-1211 Geneva 20
Switzerland

Telephone +41 22 730 5111
Telefax Gr3: +41 22 733 7256
Gr4: +41 22 730 6500

Date: 22 May 2008

Page 1/5 **Ref:**

To : ITU Member States, Sector Members and Associates of the Asia-Pacific Region

Fax:

For your reply:

Contact: Mr Wisit Atipayakoon
ITU Regional Office for Asia and the Pacific

E-mail: wisit.atipayakoon@itu.int
Fax: +66 2 574 9328 Tel.: +66 2 574 8565

Ms Christine Sund
ICT Applications and Cybersecurity Division
Policies and Strategies Department

E-mail: cybmail@itu.int
Fax: +41 22 730 5484 Tel.: +41 22 730 5203

Subject: ITU Regional Cybersecurity Forum for Asia-Pacific and Seminar on the Economics of Cybersecurity, Brisbane, Australia, 15-18 July 2008

Dear Sir/Madam,

On behalf of the International Telecommunication Union (ITU), we would like to invite you to participate in the ITU Regional Cybersecurity Forum for Asia-Pacific, to be held between 15 and 18 July 2008 in Brisbane, Australia. The meeting is being hosted by the Department of Broadband, Communications and the Digital Economy (DBCDE), Government of Australia.

The purpose of the Forum is to identify the main challenges faced by countries in the region in developing frameworks for cybersecurity and CIIP, to consider best practices, share information on development activities being undertaken by ITU as well as other entities, and review the role of various actors in promoting a culture of cybersecurity.

At the start of the 21st century, modern societies have a growing dependency on information and communication technologies (ICTs) that are globally interconnected. This interconnectivity creates interdependencies and risks that must be managed at national, regional and international levels. At the national level, each nation should consider organizing itself to take coordinated action related to the prevention of, preparation for, response to, and recovery from cyber incidents. Such action require coordination and cooperation among national participants, including, those in government, business, and other organizations, as well as individual users, who develop, own, provide, manage, service and use information systems and networks. The formulation and implementation by all nations of a national framework for cybersecurity and critical information infrastructure protection (CIIP) represents a first step in addressing the challenges arising from globally interconnected ICT infrastructures.

This meeting, one in a series of regional events organized by ITU-D, is being held in response to the ITU Plenipotentiary Resolution 130: ***Strengthening the role of ITU in building confidence and security in the use of information and communication technologies*** (Antalya, 2006) and the 2006 World Telecommunication Development Conference Doha Action Plan establishing ITU-D Study Group Question 22/1: ***Securing information and communication networks: Best practices for developing a culture of cybersecurity***.

As part of this activity, ITU-D is developing a Report on Best Practices for a National Approach to Cybersecurity which outlines a Framework for Organizing a National Approach to Cybersecurity identifying five key elements of a national effort, including: 1) Developing a national cybersecurity

strategy; 2) Establishing national government-industry collaboration; 3) Creating a national incident management capability; 4) Deterring cybercrime; and 5) Promoting a national culture of cybersecurity. The Framework aims to identify the major cybersecurity actors in a country, their roles and means of coordination, interaction, and cooperation. These actors include agencies and institutions that:

- Lead government interagency efforts on cybersecurity and provide operational guidance;
- Interact with the private sector with regards to cybersecurity whether for cybercrime, incident management, or technical and policy development;
- Develop and enforce laws related to cybersecurity;
- Coordinate action related to the prevention of, preparation for, response to, and recovery from cyber incidents; and,
- Promote a national culture of cybersecurity, including awareness-raising for individuals, small businesses and other users.

This event is expected to bring together government representatives, industry actors, and other stakeholder groups in countries from the Asia-Pacific region to discuss, share information, and collaborate on the elaboration and implementation of national policy, regulatory and enforcement frameworks for cybersecurity and CIIP. It will benefit information and communication policy makers from ministries and government departments; institutions and departments dealing with cybersecurity policies, legislation and enforcement; and representatives from operators, manufacturers, service providers, industry and consumer associations involved in promoting a culture of cybersecurity.

The meeting will also consider initiatives at the regional and international level to increase cooperation and coordination amongst different stakeholders. In addition, the meeting will address, through separate sessions, some of the unique cybersecurity related challenges faced by Small Island Developing States including the Pacific Island countries. This is in line with WTDC Resolution 17 (Doha, 2006), which includes the Asia-Pacific Regional Initiative on “Unique Telecommunication / ICT Needs of the Small Island Developing States and Pacific Island Countries.”

The meeting will be conducted in English only. Practical information on the meeting, including on registration, fellowship and meeting schedule is found in annex.

Additional information is also available at **www.itu.int/ITU-D/cyb/events/2008/brisbane/**. We encourage you to consult this website, including information on the ITU National Cybersecurity/CIIP Self-Assessment Toolkit, before the meeting.

You might also wish to note that the first day of the event, 15 July 2008, will be dedicated to a **Seminar on the Economics of Cybersecurity**.

We look forward to your active participation and invaluable contribution.

Yours sincerely,

[*Signed*]

Sami Al Basheer Al Morshid

Director

Annexes: 2

Annex I
Draft Timetable

The first day of the event, 15 July 2008, will be dedicated to an ITU Tariff Group for Asia and Oceania (TAS) Seminar on the Economics of Cybersecurity.

SEMINAR ON THE ECONOMICS OF CYBERSECURITY	
TUESDAY 15 JULY 2008	
08:00–09:00	**Meeting Registration**
09:00–09:15	**Meeting Opening and Welcome**
	Welcoming Address: Representative from the ITU Tariff Group for Asia and Oceania (TAS) *Opening Remarks:* Seminar Chairperson
09:15–10:15	**Session 1: The Economics of Cybersecurity – An Introduction**
10:15–10:30	**Coffee/Tea Break**
10:30–12:00	**Session 2: The Financial Aspects of Network Security: Malware and Spam**
12:00–13:30	**Lunch**
13:30–14:45	**Session 3: The Botnet Economy**
14:45–15:00	**Coffee/Tea Break**
15:00–16:30	**Session 4: Elaboration and Development of Indicators for Cybersecurity**
16:30–17:00	**Seminar Wrap-Up and Conclusions**

ITU REGIONAL CYBERSECURITY FORUM FOR ASIA-PACIFIC	
WEDNESDAY 16 JULY 2008	
08:00–09:00	**Meeting Registration**
09:00–10:15	**Meeting Opening and Welcome**
	Welcoming Address: Representative from Australia *Opening Remarks:* Representative from ITU *Presentation:* Setting the Stage — The Changing Cybersecurity Threat Environment
10:15–10:30	**Coffee/Tea Break**
10:30–12:00	**Session 1: Towards a Framework for Cybersecurity and Critical Information Infrastructure Protection**
12:00–13:30	**Lunch**

13:30–15:15	Session 2: Management Framework for Organizing National Cybersecurity/CIIP Efforts: Promoting a Culture of Cybersecurity
15:15–15:30	Coffee/Tea Break
15:30–17:00	Session 3: Management Framework for Organizing National Cybersecurity/CIIP Efforts and Country Case Studies: Government—Industry Collaboration
17:00–17:15	Daily Wrap-Up and Announcements
18:00–	Welcome Reception (TBC)
THURSDAY 17 JULY 2008	
09:00–10:30	Session 4: Management Framework for Organizing National Cybersecurity/CIIP Efforts and Country Case Studies: Legal Foundation and Enforcement
10:30–10:45	Coffee/Tea Break
10:45–12:00	Session 5: Management Framework for Organizing National Cybersecurity/CIIP Efforts and Country Case Studies: Incident Management Capabilities
12:00–13:30	Lunch
13:30–15:00	Session 6: Management Framework for Organizing National Cybersecurity/CIIP Efforts and Country Case Studies: Developing a National Cybersecurity Strategy
15:00–15:15	Coffee/Tea Break
15:15–17:00	Session 7: Review and Discussion: Management Framework for Organizing National Cybersecurity/CIIP Efforts
17:00–17:15	Daily Wrap-Up and Announcements
18:00-	Social Event (TBC)
FRIDAY 18 JULY 2008	
09:00–10:30	Session 8: Cybersecurity and Small Island Developing States (SIDS)
10:30–10:45	Coffee/Tea Break
10:45–12:30	Session 9: Cybersecurity and Small Island Developing States (SIDS) (Continued)
12:30–14:00	Lunch
14:00–15:30	Session 10: Regional and International Cooperation
15:30–15:45	Coffee/Tea Break
15:45–16:45	Session 11: Wrap-Up, Recommendations and the Way Forward
16:45–17:00	Meeting Closing
	Closing remarks: Representative from Australia *Closing remarks:* Representative from ITU

Annex II

Australian Government
Department of Broadband, Communications and the Digital Economy

International Telecommunication Union

ITU Regional Cybersecurity Forum for Asia-Pacific and Seminar on the Economics of Cybersecurity

15-18 July 2008
Brisbane, Australia

Pre-Registration and Fellowships Requests

Meeting participation is open to ITU Member States, Sector Members, Associates, and other interested stakeholders, including representatives from regional and international organizations.

We are pleased to inform you that ITU will provide one full fellowship for each delegation duly authorized by their respective ITU Administration in the least developed countries (LDCs) in the Asia-Pacific region, subject to available budget, for participating in this meeting. The number of delegates from a country is not limited, however, the country will bear all costs of additional delegates. Ideally a country would send representatives reflecting the major functions in cybersecurity referenced in the bulleted points above. It is expected that each delegation be familiar with their national cybersecurity-related initiatives.

The meeting pre-registration and fellowships form can be found at
www.itu.int/ITU-D/cyb/events/2008/brisbane/registration

Registrations and applications for fellowships should be made as soon as possible, but not later than 15 June 2008. Countries requiring assistance to attend the meeting should contact Mr. Wisit Atipayakoon at the ITU Regional Office for Asia and the Pacific in Bangkok, Thailand, on telephone: +66 2 574 8565 or e-mail: **wisit.atipayakoon@itu.int** with copy to **cybmail@itu.int**.

Contributions

Electronic contributions to the meeting on national cybersecurity experiences are solicited. Please send these to **cybmail@itu.int** before 20 June 2008.

Draft Forum Agenda

The full agenda with a short description of the content of each session can be found at
www.itu.int/ITU-D/cyb/events/2008/brisbane/brisbane-agenda.pdf

Practical Information for Meeting Participants

Practical information for participants is available at
www.itu.int/ITU-D/cyb/events/2008/brisbane/brisbane-practical-information.pdf