Common Market
for Eastern and Southern Africa

International Telecommunication Union

Date: 9 June 2008 **Page 1/5** Ref: **DM-154**

To : COMESA Member States, ITU Member States, Sector Members and Associates in Eastern and Southern Africa.

Fax: See list.

For your reply:

Contact: Mr Marcelino Tayob
ITU Area Office in Harare, Zimbabwe

E-mail: marcelino.tayob@itu.int
Fax: +263 4 775939 Tel.: + 263 4 771257

Mr Abu Sufian E Dafalla
Common Market for Eastern and Southern Africa (COMESA)

E-mail: ADafalla@comesa.int
Fax: +260 211 229725 Tel.: +260 211 225107

Ms Christine Sund
ICT Applications and Cybersecurity Division
BDT Policies and Strategies Department/ITU

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

Subject: ITU Regional Cybersecurity Forum for Eastern and Southern Africa held in Lusaka, Zambia, 25-28 August 2008

Dear Sir/Madam,

It is with great pleasure that we invite you to participate in the upcoming **ITU Regional Cybersecurity Forum for Eastern and Southern Africa** jointly organized by Common Market for Eastern and Southern Africa (COMESA) and the International Telecommunication Union (ITU) and hosted by the Communications Authority of Zambia (CAZ), Republic of Zambia, to be held between 25 and 28 August 2008 in the Protea Hotel Safari Lodge, about 35 km from Lusaka, Republic of Zambia.

The purpose of the Forum is to identify the main challenges faced by countries in the region in developing frameworks for cybersecurity and Critical Information Infrastructure Protection (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. The event aims to bring together government representatives, industry actors, and other stakeholder groups in countries in Eastern and Southern Africa to discuss, share information, and collaborate on the elaboration and implementation of national policy, regulatory and enforcement frameworks for cybersecurity and CIIP. It will also benefit the information and communication policy makers from ICT and justice ministries and government departments; institutions and departments dealing with cybersecurity policies, legislations and enforcement; and representatives from operators, manufacturers, service providers, industry and consumer associations involved in promoting a culture of cybersecurity.

During the four days of the Forum the participants will look at the cybersecurity issues emanated from modern societies' 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 requires 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 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.

The meeting will also consider initiatives at the regional and international level to increase cooperation and coordination amongst different stakeholders. The forum programme will include an interactive session on the ITU National Cybersecurity/CIIP Self-Assessment Toolkit, and we look forward to active participation of the delegates in this exercise.

The workshop will be conducted in English and French with simultaneous interpretation. Participation in the Forum is open to all ITU and/or COMESA Member States, Sector Members, Associates, and other interested stakeholders, including representatives from regional and international organizations. A draft forum timetable is enclosed and more detailed information about the event, including on registration, fellowship and meeting schedule is found in the annexes. Additional information is also available on the event website at www.itu.int/ITU-D/cyb/events/2008/lusaka/. We encourage you to consult this website, including the information on the ITU National Cybersecurity/CIIP Self-Assessment Toolkit, before the meeting.

We look forward to your active participation and invaluable contribution to this event.

Yours sincerely,

For COMESA	For ITU
[*Original signed*] Sindiso Ngwenya Secretary General. a. i.	[*Original signed*] Sami Al Basheer Al Morshid Director, Telecommunication Development Bureau

Annexes: 2

Annex I

Pre-Registration and Fellowship Applications

Forum participation is open to all ITU and/or COMESA Member States, Sector Members, Associates, and other interested stakeholders, including representatives from regional and international organizations.

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

We are pleased to inform you that ITU will provide one fellowship for each eligible delegation duly authorized by their respective ITU Administration in the least developed countries (LDCs) in the Eastern and Southern Africa region, subject to available budget, for participating in this meeting. In addition, COMESA will provide one fellowship for each eligible COMESA Member State. The fellowship includes an economy class air return ticket and subsistence allowance for the duration of the event. The fellowships are primarily targeted at regulatory authorities and ICT Ministries. The fellowship applicants should themselves meet the cost of any additional charges related to, but not limited to, transit nights and entry visa fees. Please send in your sponsored nominees before **31 July 2008** using the online Fellowship Request Form available at **www.itu.int/ITU-D/cyb/events/2008/lusaka/registration/**.

The number of delegates from each country participating in the meeting is not limited but each additional delegate will have to bear the full costs of his/her participation. 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.

Registrations and fellowship applications should be made as soon as possible, but not later than 31 July 2008.

Countries requiring assistance to attend the meeting should contact Mr. Marcelino Tayob in the ITU Area Office in Harare, Zimbabwe on telephone: +263 4 775939or e-mail: marcelino.tayob@itu.int with copy to cybmail@itu.int. Additional information about the event can also be provided by Dr. Abu Sufian E Dafalla (e-mail: ADafalla@comesa.int) or Ms. Christine Sund, (e-mail: christine.sund@itu.int)

Contributions

Electronic contributions to the meeting on national experiences are solicited. We encourage you to send these contributions to cybmail@itu.int before **31 July 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/lusaka/agenda.html**

Practical Information for Meeting Participants

Practical information for participants is available at **www.itu.int/ITU-D/cyb/events/2008/lusaka/practical-information.html**

Annex II

Draft Timetable

ITU Regional Cybersecurity Forum for Eastern and Southern Africa

25-28 August 2008
Lusaka, Zambia

ITU REGIONAL CYBERSECURITY FORUM FOR EASTERN AND SOUTHERN AFRICA	
MONDAY 25 AUGUST 2008	
08:00–09:00	Meeting Registration
09:00–10:15	Meeting Opening and Welcome
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 and Country Case Studies: 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 (To be confirmed)
TUESDAY 26 AUGUST 2008	
09:00–10:15	Session 4: Management Framework for Organizing National Cybersecurity/CIIP Efforts and Country Case Studies: Legal Foundation and Enforcement
10:15–10:30	Coffee/Tea Break
10:30–12:00	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 (To be confirmed)

WORKING SESSIONS ON DEVELOPING NATIONAL AND REGIONAL CYBERSECURITY/CIIP CAPACITY

WEDNESDAY 27 AUGUST 2008

09:00–11:00	Working Session 1: Legal Foundation and Enforcement
11:00–11:15	Coffee/Tea Break
11:15–12:30	Working Session 2: Legal Foundation and Enforcement
12:30–14:00	Lunch
14:00–15:30	Working Session 3: Developing a National Cybersecurity Strategy
15:30–15:45	Coffee/Tea Break
15:45–16:45	Working Session 4: Developing a National Cybersecurity Strategy
16:45–17:00	Daily Wrap-Up and Announcements

THURSDAY 28 AUGUST 2008

09:00–11:00	Session 8: ITU National Cybersecurity/CIIP Self-Assessment Toolkit: An Exercise
11:00–11:15	Coffee/Tea Break
11:15–12:30	Session 9: ITU National Cybersecurity/CIIP Self-Assessment Toolkit: An Exercise (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