INTERNATIONAL TELECOMMUNICATION UNION

Telecommunication
Development Bureau

T E L E F A X

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: 4th October 2007 Page 1/9 Ref: DM-302

To : ITU Member States, Administrations/Regulators, Sector Members, Associate Members, in Africa Region Fax: See attached list

For your reply:

Contact: Mrs. Margarida Evora Sagna
ITU Area Office for West Africa

E-mail: margarida.evora@itu.int

Fax: +221 8228013 Tel.: +221 849 77 20

Mr. Robert Shaw
ICT Applications and Cybersecurity Division
Policies and Strategies

E-mail: cybmail@itu.int

Fax: +41 22 730 5484 Tel.: +41 22 730 5338

Subject: West Africa Workshop on Policy and Regulatory Frameworks for Cybersecurity and CIIP in Praia, Cape Verde, 27-29 November 2007

Dear Sir/Madam

On behalf of the International Telecommunication Union (ITU), we would like to invite you to participate in the **West Africa Workshop on Policy and Regulatory Frameworks for Cybersecurity and Critical information infrastructure protection (CIIP)**, to be held 27-29 November 2007 in Praia, Santiago Island, Republic of Cape Verde. The workshop is being hosted by the *Cape Verde Ministry of Transports and Infrastructures* and organized in collaboration with the Regulatory Body of Cape Verde, *Agência Nacional das Communicações (ANAC)*.

The integration of information and communication technologies (ICTs) into almost every sphere of daily economic and social activity has increased the dependencies of individuals, organizations and governments on globally interconnected networks. The rapid growth in the use of ICTs during the last decade and a rising number of cyber incidents and fraudulent activities have led to a significant shift in the perception of the importance of cybersecurity. This has been further enforced by a growing understanding of the close linkage between cybersecurity and CIIP.

In order to promote cybersecurity and protect critical networked infrastructures, coordinated national action is required to prevent, respond to and recover from incidents. National frameworks and strategies are needed that allow stakeholders (individuals, organizations and governments) to use all the technical, legal and regulatory tools available to promote a culture of cybersecurity — along with regional and international cooperation. This workshop aims to bring together government representatives, industry actors, and other stakeholder groups in West-African countries 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 workshop will also consider initiatives on the regional and international level to increase cooperation and coordination amongst different stakeholders.

Workshop participation is open to ITU Member States, Sector Members, Associate Members, and other interested stakeholders, including representatives from regional and international organizations. A limited number of fellowships will be granted to participants from LDCs. To apply for fellowship, please return annex 3 (Fellowship request form) to ITU Geneva by fax: +41 22 730 5778.

The workshop will be conducted in English, French and Portuguese with simultaneous interpretation. A draft workshop agenda is enclosed and more detailed information about the event is available at www.itu.int/ITU-D/cyb/events/2007/praia/. Electronic contributions to the meeting on national experiences are solicited.

Participants who require assistance to attend the workshop should contact Ms. Anna Barboza by e-mail: anna.barboza@itu.int or by fax: + 221 8228013. The workshop registration form should be sent to Ms. Anna Barboza at the ITU Area Office, Dakar, Senegal with a copy to Agência Nacional de Comunicações (ANAC) by fax: +238 2613069, as soon as possible, but not later than 20 October 2007.

We look forward to your active participation and invaluable contribution.

Accept, Sir, Madam, the assurances of my highest consideration.

Sami Al Basheer Al Morshid
Director

[original signed]

Enclosures:

- Draft Agenda (Annex 1)
- Pre-Registration Form (Annex 2)
- Fellowship Request Form (Annex 3)
- Practical Information for Meeting Participants (Annex 4) (also available online at www.itu.int/ITU-D/cyb/events/2007/praia/).

ANNEX 1

West Africa Workshop on Policy and Regulatory Frameworks for Cybersecurity and CIIP

27-29 November 2007
Praia, Cape Verde

Draft Agenda

Description: The integration of information and communication technologies (ICT) into almost every sphere of daily economic and social activity has increased the dependencies of individuals, organizations and governments on globally interconnected networks. The rapid growth in the use of ICTs during the last decade along with a rising number of cyber-incidents and fraudulent activities, have led to a shift in the perception of the importance of cybersecurity. This has been further enforced by a growing linkage between cybersecurity and critical information infrastructure protection (CIIP).

In order to promote cybersecurity and protect critical networked infrastructures, coordinated national action is required to prevent, respond to and recover from incidents. National frameworks and strategies are needed that allow stakeholders (individuals, organizations and governments) to use all the technical, legal and regulatory tools available to promote a culture of cybersecurity — along with regional and international cooperation.

This workshop aims to bring together government representatives, industry actors, and other stakeholder groups in the West-Africa 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 workshop will also consider initiatives on the regional and international level to increase cooperation and coordination amongst different stakeholders.

TUESDAY 27 NOVEMBER 2007	
08:00–09:00	**Meeting Registration**
09:00–10:15	**Meeting Opening and Welcome**
	Welcoming Address: Cape Verde Administration/ Ministério das Infraestruturas e Transportes, Cape Verde ***Opening remarks:*** ITU-D Representative
10:15–10:30	**Coffee/Tea Break**
10:30–12:00	**Session 1: Creating a National Strategy and Framework for Cybersecurity and Critical Information Infrastructure Protection (CIIP) - Overview**
	Session Description: The necessity of building confidence and security in the use of ICTs, promoting cybersecurity and protecting critical infrastructures at national levels is generally acknowledged. As national public and private actors bring their own perspective to the relevant importance of issues, in order to have a consistent approach, some countries have established institutional

	cybersecurity/CIIP frameworks. This session reviews, from a broad perspective, different approaches to such frameworks and their often similar components in order to provide participants with a broad overview of the issues and challenges involved.
12:00–13:30	**Lunch**
13:30–15:00	**Session 2: Development of a National Strategy for Cybersecurity and Critical Information Infrastructure Protection (CIIP)**
	Session Description: Increasingly, electronic networks are being used for criminal purposes, or for objectives that can harm the integrity of critical infrastructure and create barriers for extending the benefits of ICTs. To address these threats and protect infrastructures, each country needs a comprehensive action plan that addresses technical, legal and policy issues, combined with regional and international cooperation. What issues should be considered in a national strategy for cybersecurity and critical information infrastructure protection? Which actors should be involved? Are there examples of frameworks that can be adopted? This session seeks to explore in more detail various approaches, best practices, and identify key building blocks that could assist countries in West-Africa in establishing national strategies for cybersecurity and CIIP.
15:00–15:15	**Coffee/Tea Break**
15:15–17:00	**Round Table Information Exchanges on a Framework for Cybersecurity and Critical Information Infrastructure Protection and the Development of a National Strategy**
17:00–17:15	**Daily Wrap-Up and Announcements**

WEDNESDAY 28 NOVEMBER 2007	
09:00–10:15	**Session 3: Legal Foundation and Regulatory Development**
	Session Description: Appropriate legislation, international legal coordination and enforcement are all important elements in preventing, detecting and responding to cybercrime and the misuse of ICTs. This requires updating of criminal law, procedures and policy to address cybersecurity incidents and respond to cybercrime. As a result, many countries have made amendments in their penal codes, or are in the process of adopting amendments, in accordance with international conventions and recommendations. This session reviews some various national legal approaches and potential areas for international legal coordination efforts.
10:15–10:30	**Coffee/Tea Break**
10:30–12:00	**Session 4: Legal Foundation and Regulatory Development (continued)**
	Session Description: see above
12:00–13:30	**Lunch**
13:30–15:00	**Session 5: Legal Foundation and Regulatory Development (continued)**
	Session Description: see above
15:00–15:15	**Coffee/Tea Break**
15:15–17:00	**Round Table Information Exchanges on a Legal Foundation and Regulatory Development for Enhanced Cybersecurity**
17:00–17:15	**Daily Wrap-Up and Announcements**

THURSDAY 29 NOVEMBER 2007	
09:00–10:15	**Session 6: Watch, Warning and Incident Response Capabilities**
	Session Description: A key activity for addressing cybersecurity at the national level requires preparing for, detecting, managing, and responding to cyber incidents through establishment of watch, warning and incident response capabilities. Effective incident management requires consideration of funding, human resources, training, technological capability, government and private sector relationships, and legal requirements. Collaboration at all levels of government and with the private sector, academia, regional and international organizations, is necessary to raise awareness of potential attacks and steps toward remediation. This session discusses best practices and related standards in the technical, managerial and financial aspects of establishing national or regional watch, warning, and incident response capabilities.
10:15–10:30	**Coffee/Tea Break**
10:30–12:00	**Session 7: Countering Spam and Related Threats**
	Session Description: One of the more prominent risks to Internet security is spam, which has mutated from a general annoyance to a broader cybersecurity threat. Spam is now the primary mechanism for delivering viruses that can hijack millions of computers (e.g. botnets) or launching phishing attacks to capture private or corporate financial information. Spam also acts as a platform for many other types of scams. A number of counter-measures against spammers – technical, legal, financial, user training - can be used, but there is a general lack of overall coordination at the international level. This session looks at some of the standards, best practices and initiatives that have been launched to counter spam and related threats.
12:00–13:30	**Lunch**
13:30–14:45	**Session 8: Regional and International Cooperation**
	Session Description: Regional and international cooperation is extremely important in fostering a culture of security, along with the role of regional fora to facilitate interactions and exchanges. This session will review some of the ongoing regional and international cooperation initiatives in order to encourage meeting participants to participate in further concrete actions that could be implemented in the West Africa region and internationally.
14:45–15:00	**Coffee/Tea Break**
15:00–16:00	**Session 9: Wrap-Up, Recommendations and the Way Forward**
	Session Description: The final session of the meeting reports some of the main findings from the even. It will review some of the ongoing regional and international cooperation initiatives in order to encourage meeting participants to participate in further concrete actions that could be implemented in the region and internationally. The recommendations that are elaborated upon in this session aim to set the direction for future activities in order to enhance cybersecurity and increase protection of critical information infrastructures in the region.
16:00–16:15	**Meeting Closing**
	Closing remarks: Cape Verde Administration/ Ministério das Infraestruturas e Transportes, Cape Verde ***Closing remarks:*** ITU-D Representative

ANNEX 2

West Africa Workshop on Policy and Regulatory Frameworks for Cybersecurity and CIIP

Praia, Cape Verde, 27 - 29 November 2007

PRE-REGISTRATION FORM

Form to be returned to
ITU Area Office for West Africa, Dakar, Senegal by email: anna.barboza@itu.int or by fax: + 221 822 80 13
with a copy to ANAC, Cape Verde by fax: +238 261 30 69, by **20 October 2007**

1. Mr./ Ms.
_____
(family name) (first name)

2. Official title: _____

3. Organization: _____

4. Address: _____

5. Country: _____ **Nationality:** _____

6. TEL: _____ **FAX:** _____ **E-MAIL:** _____

7. Passport No. : _____ **Place of Issue:** _____

8. Date of Issue: _____ **Expiry Date:** _____

9. Date of Birth: _____ **Place of Birth:** _____

10. Place of getting visa: _____
(in your country of other country on the journey)

11. Affiliation with ITU
- ☐ Administration of ITU Member State
- ☐ ITU Sector Member
- ☐ ITU Associate Member
- ☐ Non-Member

FLIGHT INFORMATION

Date of Arrival	Time of Arrival	FLIGHT NO.
Date of Departure	Time of Departure	FLIGHT NO.

HOTEL RESERVATION

Name of hotel:.....

- ☐ Single Executive Room
- ☐ Double Executive Room
- ☐ Executive Club Suites (Single)
- ☐ Executive Club Suites (Double)

Date In: _____ Date Out: _____

Date: _____	Signature:

ANNEX 3

West Africa Workshop on Policy and Regulatory Frameworks for Cybersecurity and CIIP

Praia, Cape Verde, 27 – 29 November 2007
FELLOWSHIP REQUEST FORM

Ministério das Infraestruturas e Transportes

Please return to: Head Fellowships Service
ITU, Place des Nations
CH - 1211 Genève 20, Switzerland

Tel.: +41 22 730 5487
Fax: +41 22 730 5778
christine.jouvenet@itu.int

WOMEN CANDIDATES ARE ENCOURAGED

FELLOWSHIP REQUEST TO BE SUBMITTED BY 20 October 2007
(Please print/type clearly)

Country _____ The Administration /Organization _____

Family name Ms./Mrs/Mr._____ Given name(s) _____

Present Post (job title): _____

Professional mailing address: _____

_____

Telephone: _____ Fax: _____

E-mail (print clearly) _____

CANDIDATE'S PERSONAL DETAILS:

PASSPORT INFORMATION:

Place and Date of Birth: _____

Nationality _____ Passport number _____

Date passport issued_____ Place of issue _____

Valid until (date) _____

CONDITIONS: Fellowships are awarded under the following conditions:

1. One fellowship per eligible country.
2. Full fellowship for LDCs and partial fellowship (DSA only) for other eligible countries.
3. A daily allowance to cover cost of board/lodging and miscellaneous expenditure.
4. It is imperative that participants awarded ITU fellowships be present from the first day and participate during the entire fellowship period.

Place, date & signature of fellowship candidate _____

TO VALIDATE FELLOWSHIP REQUEST, NAME AND SIGNATURE OF RESPONSIBLE ADMINISTRATION OFFICIAL MUST BE COMPLETED BELOW, WITH OFFICIAL STAMP:

Name and title of official in block capitals: _____

Signature of certifying official: _____ **Date:** _____

ANNEX 4

PRACTICAL INFORMATION FOR MEETING PARTICIPANTS

West Africa Workshop on Policy and Regulatory Frameworks for Cybersecurity and CIIP

Praia, Cape Verde, 27 – 29 November 2007

Ministério das Infraestruturas e Transportes

1 Venue

The workshop will be held at **Praia Mar Hotel**

Address: Praia Mar Hotel
CP 75 Prainha
Praia – SANTIAGO
CAPE VERDE

Tel: +238 261 37 77
Fax:+238 261 29 72

E-mail: praiamar@cvtelecom.cv

2 Getting to Praia, Cape Verde

There are regular direct flights from Dakar, Lisbon, Paris, and less frequent flights from other European and African cites to Praia, Cape Verde.

3 Arrival and local transportation

Please note that workshop participants should arrange their own transportation from the airport to their respective hotels, some hotels can provide shuttle buses.

4 Entry requirements for Cape Verde

A valid passport and visa are required to enter Cape Verde. Except, nationals from ECOWAS countries. Participants are, therefore, requested to contact the Cape Verde embassy in their country to obtain the visa. Any participant who may encounter difficulties in obtaining a visa are requested to get in touch with Agencia Nacional das Communicaçoes (ANAC), Tel.: +238 260 44 00, or fax +238 2613069.

4 Currency

The Cap Verdian currency is the Escudos. The current exchange rate is 1 EURO = 110 escudos and 1 USD = 80 escudos. Change can be made in the banks and exchange offices.

5 Electricity

The main voltage is 220 volts / 50 Hz. For lower voltage, check with the hotel reception.

6 Climate

Cape Verde is located in West Africa (and in the Northern Tropical area). The workshop takes place during the dry season, when the temperature is around 24°C and humidity is low.

7 Health and vaccinations

An international vaccination certificate is required for yellow fever.

8 Contact

For further information, please contact:

Mrs Manuela Pereira

Tel.: +238 2604400

Fax: +238 2613069

E-mail: manuela.pereira@anac.cv

9 Accommodation

A list of recommended hotels offering preferential tariffs is provided below.

LIST OF RECOMMENDED HOTELS AND RESIDENCIALS

HOTEL	SINGLE ROOMS		DOUBLE ROOMS		TELEPHONE	FAX	EMAIL
	ESCUDOS	EUROS	ESCUDOS	EUROS			
Hotel Praia Mar **** (event venue)	11.250	102	14.110	128	+238 260 84 40	+238 261 29 72	praiamar@cvtelecom.cv
Hotel Tropico ****	10.900	99	13.790	122	+238 261 42 00	+238 261 52 25	hotel.tropico@cvtelecom.cv
Pérola ***	4.455	42	5.850	55	+238 260 14 40	+238 261 14 48	perola@cvtelecom.cv
Eurolines ***	3.500	30	-	-	+238 260 30 10	+238 261 66 60	Eurolines@cvtelecom.cv
Residencial Praia-Maria ***	4.770	46	5.600	57	+238 26175 23	+238 261 85 54	res.praiamaria@cvtelecom.cv
Residencial Bera Mar***	4.950	45	6.930	63	+238 261 64 00	+238 261 30 69	beramar@cvtelecom.cv