PCC.I/DEC. 125 (XIX-11) [1]

QUESTIONNAIRE ON THE CURRENT STATUS OF NATIONAL MEASURES AGAINST THEFT OF MOBILE TERMINAL EQUIPMENT

The XIX Meeting of the Permanent Consultative Committee I: Telecommunications/ Information and Communication Technologies (PCC.I),

DECIDES:

1. To instruct the Executive Secretary of CITEL to forward to the Administrations the questionnaire contained in the Annex below and to transmit the replies to said questionnaire to the Rapporteurs on Regulatory non-compliance Practices and fraud Control in telecommunications/ICT.

2. To request the Administrations to complete the questionnaire and return it by October 21, 2011 at the latest, by email to the Secretariat of CITEL (citel@oas.org).

ANNEX TO DECISION PCC.I/DEC. 125 (XIX-11)

CURRENT STATUS OF NATIONAL MEASURES AGAINST THEFT OF MOBILE TERMINAL EQUIPMENT

Country / Administration: _________________________

Sent by: ___________________________

Entity / Institution __________________

Contact:

Telephone _______________________ E-mail _____________________

List of measures against the theft of cellular equipment. Please indicate those measures implemented in your country. If measures have been implemented, please indicate, insofar as possible, how they have been implemented.

[1] CCP.I-TIC/doc. 2362/11 rev.3

No.	QUESTION	ANSWER	
		YES	NO
1	Prohibition of activation on the cellular network of IMEI reported stolen/lost (international Mobile Equipment Identification)		
2	Blocking in sales and activation systems of devices reported stolen/lost		
3	Exchange of negative lists (blacklists) between operators in the country		
4	Regulatory obligation for operators to prohibit activation		
5	Centralized database of stolen equipment		
6	Exchange of blacklist databases with other countries		
7	Connection to regional blacklist databases		
8	Connection to the GSM Association (GSMA) IMEI DB (Global EIR) (Database of GSMA IMEI previously known as Global EIR or Global Equipment Identity Register)		
9	Control of informal sales of mobile terminal equipment		
10	Security assessment of terminal devices at time of purchase in accordance with the GSMA's IMEI security principles		
11	Use of the GSMA service for reporting vulnerabilities in the security of IMEIs of mobile terminal devices		
12	Sanctions of imprisonment for reprogramming the IMEI of a mobile terminal device		
13	Public campaigns to raise awareness of measures against the theft of mobile terminal devices		
14	Import controls of uncertified mobile terminal devices used or reported stolen		
15	Controls on the exit or re-export of used/stolen mobile terminal devices		
16	Suspension or prohibition of activation of the Personal Identification Number of chat services of smartphone manufacturers for devices reported stolen/lost		
17	Are user requirements in place for mobile terminal devices prior to online activation other than those established by the mobile operator?		
18	There provisions to suspend or prohibit the activation of invalid IMEIs (IMEIs not 15 digits in length, or whose TAC does not correspond to the make and model assigned by the GSM Association (GSMA), and/or duplicate IMEIs (the same IMEI programmed into more than one mobile terminal device)		