

## PCC.I/DEC. 284 (XXXIII-18)<sup>1</sup>

### **SUBMISSION OF DRAFT RESOLUTION FOR THE OAS GENERAL ASSEMBLY “HEMISPHERIC EFFORTS TO COMBAT THE USE OF STOLEN, LOST OR TAMPERED MOBILE TERMINAL DEVICES” TO THE 35 MEETING OF COM/CITEL”**

The 33 Meeting of the Permanent Consultative Committee I: Telecommunications/Information and Communication Technologies (PCC.I),

#### **DECIDES:**

- 1) To submit the Draft Resolution on “Hemispheric Efforts to Combat the Use of Stolen, Lost or Tampered Mobile Terminal Devices”, attached to this Draft Decision, to the 35 Meeting of the Permanent Executive Committee COM/ CITEL, for discussion and approval, so that it can be submitted for approval at the 49 Regular Session of the OAS General Assembly.
- 2) To instruct the Executive Secretary of CITEL to send the abovementioned Draft Resolution on “Hemispheric Efforts to Combat the Use of Stolen, Lost or Tampered Mobile Terminal Devices” to CITEL/OAS Member State Administrations, their Permanent Missions to the OAS and CITEL’s Associate Members; requesting to submit their comments by October 15, 2018. These comments will be incorporated into a working document to be drafted by the Secretariat, so that they are made available to the 35 Meeting of the Permanent Executive Committee (COM/CITEL) for discussion and adoption of a Draft Resolution that takes into consideration the consultation results.
- 3) That COM/CITEL is the CITEL body in which the text will be defined and adopted to submit to the OAS General Assembly for its approval.

#### **ANNEX TO DECISION PCC.I/DEC. 284 (XXXIII-18)**

### **DRAFT RESOLUTION FOR THE OAS GENERAL ASSEMBLY “HEMISPHERIC EFFORTS TO COMBAT THE USE OF STOLEN, LOST OR TAMPERED MOBILE TERMINAL DEVICES”**

(Approved at \_\_\_\_\_ Plenary Session held on \_\_\_\_\_)

The GENERAL ASSEMBLY,

**GIVEN** both “CITEL’s Technical Report on the use of stolen, lost or tampered mobile terminal devices” (CP/doc. xxxx/18), as well as COM/CITEL’s Conceptual Framework through which this Resolution was submitted for consideration to the Permanent Council;

---

<sup>1</sup> PCC.I-TIC/doc. 4649/18 rev.1 cor. 2

### **CONSIDERING:**

The positive impact of mobile telecommunications and the technological developments it entails has meant an increase in the penetration of smart mobile devices, which in turn has brought about a dramatic increase in device theft, in life threatening assaults and crimes resulting in injured victims, turning this into a domestic and regional citizen safety concern with deep social repercussions;

The Judiciary and law enforcement authorities, who are combating this and other crimes, have identified the actions of international criminal organizations devoted to this illegal activity, which has become a lucrative business and a way to maintain communications anonymous;

Given the efforts and progress made internally in each of the Member States to combat this crime, the illegal traffic of stolen devices and parts has increased across borders;

Technological measures, such as blocking both domestic and international mobile networks in stolen devices, are dependent on the devices' security ID, which the criminals proceed to tamper with so as to reintroduce those devices in the market, thus rendering security measures less effective;

### **BEARING IN MIND:**

that the Inter-American Telecommunication Commission - CITEL recognizes the seriousness of this issue, especially in connection with the social repercussions of mobile device theft, it has issued a document on "Regional Measures against Mobile Terminal Device Theft", within the framework of its 19 Meeting of the Permanent Consultative Committee COM/ CITEL I (Telecommunications/ Information and Communications Technologies) - PCC.I in September 2011: Resolution PCC.I/RES.189 (XIX-11). In said Resolution, among other measures, the PCC urges Member States to include provisions in their regulations to ban the activation and use of IDs reported as stolen or lost, or devices from illegal origin, included in domestic, regional or international lists;

### **RECOGNIZING:**

The efforts and progress made by the Member States, the industry (mobile manufacturers and carriers/ operators) and the Judiciary and law enforcement authorities to combat mobile device theft and tampering or duplication;

The progress made in exchange of information on and blocking of stolen devices, with partial success among Member States, using technology and databases provided by the industry; and

The fact that there are applications available to enable users to protect their personal information and render the devices useless, in case of theft or loss.

### **TAKING INTO ACCOUNT THAT**

The exchange of information on stolen or lost mobile devices, and the possibility to block them in mobile networks in all Member States is key to mitigate the consequences of this issue;

Tampering or duplication of stolen or lost devices' unique IDs evades blocking and generates an impact on manufacturers, importers, traders and users of genuine equipment, and therefore high device security standards are required to prevent such tampering, as well as to detect and block/ blacklist those devices with tampered or duplicated IDs.

It is necessary for users to adopt applications that protect their information, and enable them to render their devices useless in order to block access to internet networks and other uses.

Additionally to these technological measures, it is necessary for law enforcement, customs and Judiciary authorities to be part of this action to prevent use, sale, imports and exports of stolen, lost or tampered/ duplicated devices.

### **RESOLVES TO:**

1. Urge Member States to exchange information, block stolen or lost mobile devices that have been reported in other states, and include provisions in their regulations to ban the activation or use of such devices.
2. Invite Member States to work together with the industry in order to increase adoption of anti-theft applications among users, so as to improve device security against ID tampering.
3. Provide incentives so that Member States implement processes to detect and control mobile devices with tampered or duplicated IDs.
4. Urge Member States to strengthen their regulatory frameworks and judicial/ law enforcement actions to combat imports, exports, sale or use of stolen, lost, tampered or duplicated devices.
5. Request Member States and industrial stakeholders to collaborate and assist other Member States in the adoption, strengthening and consolidation of controls to combat the use of stolen, lost, tampered or duplicated devices.
6. Urge Member States, through their CITEL Administrations, to submit biannual reports on this specific matter. These reports shall be analyzed by the relevant CITEL Groups, and as a result of this effort, a chapter on this matter will be included in CITEL's Annual Report, highlighting the following: a) The numbers on theft and life threatening assaults or incidents with injured victims; b) Technology advances that are being implemented to discourage these crimes; and, c) Legislative measures and/or government policies passed or adopted to support public or private efforts referring to this issue.