|  |  |
| --- | --- |
| **Council 2018Geneva, 17-27 April 2018** |  |
|  |  |
|  |  |
| **Agenda item: PL 1.5** | **Document C18/76-E** |
| **3 April 2018** |
| **Original: English** |
| Report by the Secretary-General |
| Status report on Misuse of International Mobile Equipment Identity (IMEI) numbers in mobile handsets |

|  |
| --- |
| SummaryAs per Council 2017 decision, the Director of TSB communicated with the GSMA on the misuse of International Mobile Equipment Identity (IMEI) numbers in mobile handsets.Following the discussions held during the Council Working Group on Financial and Human Resources in January 2018, further exchange between the Director of TSB and GSMA took place.This report summarizes the status of the discussions and exchanges.Action requiredThe Council is invited **to note this report**.\_\_\_\_\_\_\_\_\_\_\_\_References[C17/87](https://www.itu.int/md/S17-CL-C-0087/en), [C17/124](https://www.itu.int/md/S17-CL-C-0124/en), [CWG-FHR 8/19](https://www.itu.int/md/S18-CLCWGFHRM8-C-0019/en) |

## 1. Background

A number of Member States of ITU (India, Bangladesh, Nigeria, Uganda, and Tunisia) submitted a joint contribution (C17/87 “Proposal on IMEI implementation in mobile phone handsets to address security challenges”) to the 2017 Session of Council. Currently, IMEIs are field programmable and can easily be changed, leading to security challenges and a situation where multiple mobile phones can have the same IMEI number. This is in contrast with the existing 3GPP standard TS 22.016 (International Mobile station Equipment Identities (IMEI)), which states that “[t]he IMEI shall be unique and shall not be changed after the ME’s [Mobile Equipment’s] final production process. It shall resist tampering, i.e. manipulation and change, by any means (e.g. physical, electrical and software)”, and GSMA document TS.06 (IMEI Allocation and Approval Process), which says that Type Allocation Holders have the responsibility to “[e]nsure IMEI are secure and have integrity” (clause 16).

## The summary record ([C17/124](https://www.itu.int/md/S17-CL-C-0124/en)) of the ITU Council states:

##  *“Councillors taking the floor agreed on the seriousness of the problem, in socio-economic terms and, above all, in terms of security. The problem needed to be tackled through a combination of country programmes and international cooperation initiatives, with the aim of at least ensuring that IMEI numbers were non- erasable and non-reprogrammable.” The ITU Council instructed the TSB Director “to begin collaboration with the GSMA, including highlighting the matter in a letter to GSMA, in order to resolving the problem of IMEI numbers.”*

## 2. Exchange between ITU and GSMA

The TSB Director sent a letter to the Director General of GSMA in July 2017:

*“ […] In view of the above, as an important measure of building confidence and security in the use of ICTs, ITU brings the concerns of Member States that the 3GPP standards and GSMA documents defined to protect the integrity of IMEIs are not being complied with, to the attention of GSMA, and seeks the urgent attention of GSMA and 3GPP for their cooperation with ITU and necessary action in this regard.*

*Taking this opportunity, I would like to invite you to the next meeting of ITU-T Study Group 11 to take place in Geneva from 8 to 17 November 2017. ITU-T Study Group 11 is also the lead study group on combatting counterfeiting and stolen ICT devices. Perhaps this meeting could be an occasion for an informal meeting of parties concerned to discuss the matter.*

*I look forward to continuing the fruitful cooperation with GSMA and 3GPP on this matter.”*

Following a reminder sent by the TSB Director to GSMA in December 2017, the following reply email was received from GSMA:

*“Thank you for your letter regarding the discussion at ITU Council 2017 on IMEI security. The GSMA is aware of the issue and we are already engaged with the countries involved in order to discuss how to address their concerns. We believe that we share the same view as the ITU and some Member States that IMEI security requirements are not being adhered to in all cases. It should be noted that compliance with IMEI security is the responsibility of individual device manufacturers, and not all legitimate manufacturers have security issues.*

*The GSMA will continue to work with all stakeholders and in particular with manufacturers considered to be non-compliant with security requirements. Additionally, we have recently embarked on a programme of activities to increase manufacturer awareness of the need for IMEI security and we hope to secure a renewed commitment by those manufacturers to IMEI security. Finally, the GSMA will continue to participate in ITU-T Study Group 11 and we look forward to further discussion on the matter at the next meeting in November.”*

The TSB Director reported on the matter to CWG-FHR ([CWG-FHR 8/19](https://www.itu.int/md/S18-CLCWGFHRM8-C-0019/en)) in January 2018. The subject was also discussed in CWG-Internet. Following the request of some Member States to continue to pursue the matter with GSMA and 3GPP, the TSB Director asked GSMA in February 2018 for further clarification on successful steps that GSMA has undertaken to tackle the problem of misuse of IMEI numbers:

*“Thank you for your response that we received on 18 December 2017, following my letter to you on 20 July 2017 on the misuse of IMEI numbers in mobile handsets. The matter was again discussed, including your response, at an interim meeting of Council on 25-26 January 2018. The meeting report of the Council interim meeting reads as follows (available at* [*https://www.itu.int/md/S18-RCLINTPOL11-C-0011/en*](https://www.itu.int/md/S18-RCLINTPOL11-C-0011/en)*):*

*BEGIN QUOTE*

***7.2 Discussion on document CWG-FHR 8/19 “Status report on misuse of International Mobile Equipment Identify (IMEI) numbers in mobile handsets”***

* *India requested that the report submitted by the TSB Director to CWG-FHR (Document* [*CWG-FHR 8/19*](https://www.itu.int/md/S18-CLCWGFHRM8-C-0019/en)*) be submitted to Council 2018. India stated that in their view the response received from GSMA is inadequate and requests the TSB Director to further pursue the matter.*
* *Some Member States noted that CWG-FHR and Council 2017 have already discussed the topic, and sought further clarity on the expected actions of CWG Internet on the matter.*
* *Some Member States noted that the matter concerns security in the use of ICTs, which is under the mandate of CWG Internet.*
* *Some Member States stated that TSB should continue to pursue the matter with GSMA and 3GPP within the forums, where issues related to the IMEI standards are handled.*
* *Some Member States stated that the discussed issue is not related to developing or refining standards, but to the implementation and enforcement of standards.*

*END QUOTE*

*The topic will be discussed again at the ITU Council meeting from 17 to 27 April 2018. Would it be possible that I include in my report to ITU Council successful steps that GSMA has undertaken to tackle the problem of misuse of IMEI numbers?”*

GSMA responded in March 2018:

*“[…] I would like to offer the following points:*

*1. We appreciate you informing us that the matter was discussed at an ITU Council meeting on 25-26 January 2018. A GSMA representative was in attendance during that meeting. We noted that during the Council discussion no interest was shown by Member States in discussing IMEl security. The Chair of the meeting also noted this point.*

*2. The GSMA appreciates ITU Council's recognition of 3GPP's device identifier standardisation mandate and of GSMA's role in the management and allocation of identifiers. GSMA notes the opinion of ITU Council that current concerns have less to do with standardisation and more do with and enforcement of existing standards. We would appreciate a better understanding of any proposed Council Working Group Internet (CWG-Internet) proposals in relation to lMEI.*

*3. In April, the GSMA will be launching a new lMEl Security Monitoring and Reporting Service. This outsourced service will monitor and report on IMEl implementations and collect data on security issues in handsets and on platforms that seek to modify lMEl numbers. This data will provide GSMA with the ability to address security issues in a targeted manner. We believe this will resolve any lingering concerns.*

*For more information about this new service and about the GSMA's position in relation to IMEI Security, please see the attached GSMA Briefing Note. In addition, I confirm that we continue to be willing to engage with all stakeholders, including nation states, with an interest in lMEl security. We are indeed currently in direct dialogue with India on this matter.*

*In conclusion, I would like to reiterate that the technical standard for the IMEI is held by 3GPP. Any changes to that standard should be made by the membership of 3GPP in the course of its work. The ITU does not hold the standard and its membership does not have the mandate to work on the standard. We would suggest that any concerns be addressed through participation by the ITU in the relevant 3GPP discussions”.*

The GSMA Briefing Note is available as information document (see [INF/9](http://www.itu.int/md/S18-CL-INF-0009/en)).

## 3. Conclusion

ITU members are invited to address any further concerns on IMEI security directly to GSMA and 3GPP, respectively.

The implementation of IMEI and other identifiers for combating counterfeiting and stolen ICT devices are the subject of ITU-T SG 11 standardization activities. All interested ITU members are invited to contribute to ITU-T SG11 on this matter. The next ITU-T SG11 meeting will take place in Geneva on 18-27 July 2018.