|  |  |
| --- | --- |
| **Council Working Group on  Financial and Human Resources**  **Eighth meeting – Geneva, 22-23 January 2018** |  |
|  |  |
|  |  |
|  | **Document CWG-FHR 8/19** |
| **21 December 2017** |
| **English only** |

Contribution by the Secretariat

Status report on Misuse of International Mobile Equipment Identity (IMEI) numbers in mobile handsets

|  |
| --- |
| **Background**  Following the decision highlighted in the summary record of the Council 2017 session, the Director of TSB communicated with the GSMA on the misuse of International Mobile Equipment Identity (IMEI) numbers in mobile handsets.  This report summarizes the status of such collaboration.  **Action required**  The CWG-FHR is invited to take this report into consideration.  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) |

## A. Background

## A number of ITU Member States (India, Bangladesh, Nigeria, Uganda, and Tunisia) submitted a joint contribution (C17/87 “Proposal on IMEI implementation in mobile phone handsets to address security challenges”, publicly available) to the ITU 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.”

## B. The status of collaboration 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.”*

## C. Conclusion

## All interested ITU members are invited to contribute to SG11 proposing the way forward. ITU-T, in particular ITU-T SG11 is looking forward to continuing collaboration with GSMA to address such issues.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_