ICTA

INFORMATION & COMMUNICATION
TECHNOLOGIES AUTHORITY

WSIS 2023 High-Level Policy Forum

WSIS Action Lines for building back better and accelerating the achievement of SDGs

SESSION 9

STATEMENT BY Mr Dick Ng Sui Wa
Chairman of the Information and Communication Technologies Authority, Mauritius

15 March 2023, ITU, Geneva

SECURITY AND RESILENCE OF TELECOMMUNICATION NETWORKS AS AN ENABLER FOR WATER AND ELECTRICITY DISTRIBUTION IN MAURITIUS

QUESTION 1: WHY IS SECURITY AND RESILIENCE OF TELECOMMUNICATION NETWORKS HIGH ON THE AGENDA FOR MAURITIUS, PARTICULARLY IN THE CONTEXT OF UTILITIES DISTRIBUTION?

➢ It is foreseen that utilities distribution systems will increasingly be reliant on telecommunication infrastructure, in particular 5G. Whereas in is true that these systems often have their own private network, we believe that utilities providers will find a number of operational opportunities in making use of carrier-based 5G networks. These will include the so called “Grid of Things” for electricity distribution, which will be based on the IoT capabilities of 5G. There may also be a number of advantages to migrate existing fibre based Supervisory Control and Data Acquisition (SCADA) systems over a cellular network. The viability of these changes is however dependent on a resilient and secure telecommunication network.

➢ For most of its history, the telecom industry has avoided the security scandals that have beset many industrial sectors. Subscribers have not suffered from the mass theft of private data or user identities because these cellular networks were built on proprietary physical infrastructure, and network functions resided on hardware platforms. As such in Mauritius, telecom companies have been self-regulating themselves when it comes to security standards in their network.

➢ In response to a rapid escalation in the cyber threat landscape which is inherent to IP networks, there is a pressing need to compel telecom service providers to better manage security risks not only to enhance the security and resilience of their nationwide infrastructure, but also to better manage security risks within their supply chains, especially when other critical infrastructure, such as the utilities distribution systems depend on them.

- Moreover, the current rollout of 5G networks in Mauritius makes it all the more necessary for the ICTA to come up with security regulatory framework. 5G network can potentially change the security protection enjoyed by the previous telecom network generations. This is because 5G networks are managed through software rather than hardware. The virtual nature of the 5G network core makes it vulnerable in new ways. When a network resides in software, there is a danger of cross-contamination and data leakage.

- At the international level, several countries have recently come up with specific telecom security regulations in order to handle the above issues.

- In the same vein, the ICTA intends, especially with the current 5G deployment status in Mauritius, to come up with a similar regulatory framework based on international practices, to impose on telecom operators, obligations regarding minimum network and service security requirements, risk management measures, data integrity, availability and confidentiality, and the mandatory reporting of security incidents to the ICT Authority.

- **QUESTION 2: HOW IS YOUR COUNTRY PROCEEDING TO ADDRESS THE CHALLENGES RELATED TO SECURITY AND RESILIENCE?**

- The ICTA is currently working on new Regulations and for that purpose we have requested the assistance of the Telecommunication Development Bureau (BDT) of the ITU. The objectives of these Regulations will be:

  (a) To ensure that Licensed providers of public electronic communications networks and services and their subscribers are under a regulated environment;

  (b) To ensure that providers of public electronic communications networks and services deliver same in a secured manner;

  (c) To ensure that the providers of public electronic communications networks and services protect their infrastructure and their subscribers' interests by preventing their infrastructure from being interrupted, corrupted or denied.

- The ICTA is exploring the possibility of including the GSMA Network Equipment Security Assurance Scheme (NESAS) and the Common Criteria (CC) standards in the proposed telecom network security regulations. Such an inclusion will enforce the component of the regulation dealing with the mitigation of security risks associated with third party suppliers of the telcos which is of utmost relevance for 5G mobile network equipment in line with international best practices as described below.

- From a practical standpoint, in Mauritius, such a measure will imply that imported telecom equipment will have to demonstrate compliance with the relevant schemes such as NESAS and CC in order to be type approved by the Authority for entry in the country. Hence, the type approval process will need to be amended to include a requirement for the importers to provide a certificate of compliance or independent audit reports from the relevant suppliers relating to the security of the specific network equipment.

- However, type approval process will not be able to only rely on vendor documentation unless it is possible to verify that the audit relates to the security of the specific network equipment. The proposed regulations will, therefore, need to specify that where the network equipment supplier claims to have obtained any internationally recognised security assessments such as NESAS or CC, telcos shall contractually require equipment suppliers to share with them the full findings that evidence the assessment or certificate for the specific 5G mobile network equipment to be typed approved. These full findings will, in turn, need to be shared with the ICT Authority for the type approval process.

- The Drafting of the telecom network security & resilience regulations is expected to happen in two phases in the following order:
  - (i) First there will be the Regulations pertaining to type approval process for new telecommunication equipment; and
  - (ii) Secondly, the Regulations to detail out all the security and audit requirements to ensure that adequate protection is deployed in the licensees’ network facilities.