1.0 Mr. JAMES M. KILABA's BIOGRAPHY

Mr. James M. Kilaba is currently working with Tanzania Communications Regulatory Authority (TCRA) as Director General.

Mr. Kilaba has been working in the communications sector regulation for more than 20 years. Over this period he has been a pioneer in many ICT development initiatives as well as active participant in the ITU Standardization and Development activities.

He has also been serving the ITU as ITU-T Study Group 2 Vice Chairman for two Study periods (2009–2016) and was the motivator behind the establishment of the EACO Standardization Group in East Africa.

James Kilaba is a Senior Member of the Institution of Engineers in Tanzania. He has also been a Member of the Institute of Electrical and Electronics Engineers (IEEE) for more than 15 years.

2.0 Mr. JAMES M. KILABA's INTERVENTION DURING GSS

At any ICTs discussion platforms like this, we normally don't miss talking about ICTs related Services, Devices, Growth, subscriptions or Users, Network and Signal coverage and even revenues.

Today, we are discussing the impact of emerging technologies on security, privacy and trust in ICTs. Why all these!

To me, I can just say the technological shift from an internet dominated by Personal Computers (PCs) with wired connections to the current with mobile devices connected by wireless signals has facilitated more access to communications and by extension, through Internet, to the cyber

world. And is the main cause of today's discussion! It is about ICTs related **Services**, **Devices**, **Growth**, subscriptions or **Users**, Network and Signal **coverage**.

Of course, emerging technologies in ICTs has touched all these and in total, they play a central role on **security** (*Networks, systems, devices, data and Users*), **privacy** (*data and Users*) and **trust** (*Networks, systems, devices, data and Users*).

Regulators around the world are being challenged by the role/demands of Users (**people**) and evolutions of **Devices** irrespective of where they are mounted, fitted, connected or used as far as Security, Privacy or Trust are concerned. So, it is basically the People who also have cultural diversity complemented by time-zone differences.

Now, from the perspective of developing countries, we in Tanzania have done the following:

- ✓ We have implemented our National Computer Emergency Response Team (TZ-CERT) and is used for dissemination of cyber security knowledge, information and skills to various stakeholders and Users, to be able to acquire necessary levels of expertize needed to actively tackle serious cybercrime incidents;

- ✓ We have implemented DNSSEC at our Domain Name Registry System;

- ✓ We have a newly established National Data Centre;

- ✓ We have also started to deploy mechanisms so as to prevent misuse of data or information from a stolen mobile device in the country.

And, at East African Region we have implemented Computer Emergency Response Teams (CERTs) in four countries and to a large extent we share and exchange information on cyber security incidents and threats. Through our Organization EACO, we also meet and discuss issues on the cybersecurity.

The particular challenges faced in the context of security, privacy and trust in ICTs can be listed as follows:

1. Inadequate Standards, Policies, Laws and Strategies:

- ✓ Standards, Laws and Strategies are required to improve a nation's cyber defense posture.

- ✓ As the matter does not end within one country's borders, the established Standards, Laws and Regulations need to be harmonized within regions and globally. It is believed that there are few world-class cyber experts to adequately handle cyberspace offenses and defense.

- ✓ We need National Cybersecurity Strategies that promote dissemination of cyber security knowledge, information and skills to various stakeholders and Users, to be able to acquire necessary levels of expertize needed to actively tackle serious cybercrime incidents.

2. Management of Cybersecurity – Beyond National borders:

- ✓ Some of our developing countries have no well-established and adequately equipped National Computer Incident Response Teams (CIRTs) or Computer Emergency Response Teams (CERTs).

- ✓ These kinds of facilities when well established provide national approach for coordination, analysis, responses and secure information sharing in regards to cyber security incidents and threats.

- ✓ There is a need therefore, for developing countries to have hand-shaking National-CERTs that will assist on early detection, monitoring and countering attacks, intrusions, new forms of malicious code distribution or any other type of malicious behavior.

- ✓ *Effective and collaborative management of cybersecurity is a critical capability for the defense and preservation of civil society. Cybercrime is one of the world's largest and fastest-growing categories of crime in cyberspace.*

3. Inadequate Safeguard on Critical Infrastructures:

Again some of the critical infrastructures like Domain Names Registry Systems in our countries are not well secured and therefore vulnerable to attacks.

Such kind of attacks when successful, they cause economic impact to our countries.

It is important that all critical infrastructures like Domain Names Registry Systems in our countries are properly secured and monitored.

4. **Numbering Resources Management for IoTs and M2M:**

This area is also emerging as new and therefore requiring special attention in developing countries.

5. **Inadequate education and awareness to our citizens:**

- ✓ Education to enable Users to understand issues relating to security, privacy and trust in ICT is lacking.

- ✓ This education if provided will enable users to make informed decisions on the trustworthiness of ICT applications and services including social contacts and selective information sharing.

- ✓ Unlawful use of ICTs by irresponsible Users ***Vs*** Human Rights and Privacy issues.

Let us play our part as Experts coordinated by ITU so as to mitigate the challenges paused by Security, Privacy and Trust in ICTs.

I thank you!