Welcoming remark by Heung Youl Youm, Chairman of ITU-T SG17

TSB director, Mr Seizo ONOE ,

Excellency, Deputy Minister, Ministry of Science and ICT, Republic of Korea, Dr Jin-Bae Hong,

Distinguished colleagues and participants,

Good morning, good afternoon, and good evening,

My name is Heung Youl Youm, SG17 chairman.

First of all, I sincerely thank Mr Seizo ONOE for giving us his insightful opening remarks and kind words for the workshop. I also thank Dr Jin-Bae Hong for the welcoming remark introducing Korea's activities on zero trust and software supply chain security for the workshop. I especially welcome all participants to the workshop in-person or online across the world.

It is my pleasure and honor to add my welcoming remark to this ITU workshop on "Zero trust and software supply chain security", which is now being held in Republic of Korea, my homeland, where five thousand years of history with culture and 70 years of rapid economic development are in harmony.

As you may know, ITU-T SG17 is responsible for building confidence and security in the use of ICTs by producing a set of high-quality technical standards in the area of security and data protection. Providing security by ICTs and ensuring security for ICTs are both major study areas for ITU-T Study Group 17.

Recently Zero Trust and Software Supply Chain Security have been two buzzwords for improving cybersecurity posture to defend ICT systems from the advanced, persistent, sophisticated, and well-organized cyber attacks.

Zero Trust is known as a new strategic security approach that protects enterprises by removing implicit trust and continuously evaluating every stage of digital interactions to their system. Software supply chain security focuses on the risk management during the lifecycle of the software for all related stakeholders including software vendors and users. By integrating Zero Trust principles into software supply chain security, I believe organizations can establish a strong, resilient defense system against cyber threats.

As mentioned by Dr Hong, Republic of Korean established the Forum with the intention of

formulating a new cybersecurity policy and strategy based on these two technologies in 2022 and, to my best knowledge, some other countries like the United States are leading the same direction.

The objectives of this workshop, as developed by the steering committee, include:

- providing an overview of Zero Trust and software supply chain security with insights into the new and emerging threats;
- identifying technical countermeasures and organizational controls to effectively address the identified threats;
- showcasing on-going activities among relevant ITU-T study groups and other organizations; and
- identifying a way forward and providing suggestions to ITU-T Study Group 17 on potential study topics and future direction, related to Zero Trust and software supply chain security.

Currently SG17 has two work items under development, TR.zt.acp, Guidelines for zero trust-based access control platform in telecommunication networks, in Q2/17 and X.st-ssc, Security threats of software supply chain, in Q4/17.

Moreover, SG17 has been preparing since the August/September 2022 SG17 meeting for the upcoming World Telecommunication Standardization Assembly in 2024 (known as WTSA-24) to establish new SG17 mandate and structure for the next study period (2025-2028). I am pleased to inform that this preparation activities conducted last four months agreed on those two topics, zero trust and software supply chain security, as emerging standardization topics that need to be studied in the next Study period (2025 – 2028).

I believe this is a very right time for ITU to hold this workshop for SG17 to identify the way forward from standardization's perspective to address these important topics.

I would like to conclude my remarks with the SG17 motto which I have presented at every SG17 meeting since 2017: SAFE, security is absolutely first everywhere. That means that "security by design and usage" principles should be applied to all ICT services and products from the beginning and through their lifecycle.

On behalf of SG17, as Chairman, I thank ITU for giving an opportunity for hosting this workshop in Korea and I also express my special thanks to my administration, Ministry of Science and ICT, for hosting this workshop here in KINTEX today.

I thank in advance our two masters of ceremony, Ms Yumin Jeong (News Anchor of news 8 at SBS broadcasting company in Korea) and Ms Xiaoya Yang (SG17 counsellor), four session

moderators, 22 excellent and prominent speakers for 3 sessions, and 5 panelists from across the world for the insights they bring to the workshop.

I thank 12 Steering Committee members for developing the workshop programme through multiple online meetings during past three months, and TSB event teams for their excellent support, especially to Ms Gillian Makamara, TSB project officer.

I also thank 267 pre-registered participants in person and online from 42 countries, and I hope you will find the workshop insightful and useful.

This concludes my remarks. Thank you very much.