Thank you, Mr. Chairman, for giving me the opportunity to speak and to express my sincere and growing appreciation for giving private sector stakeholder such as SafePC Solutions, the opportunity to share my feedback to some of the critical questions that you are asking –

Are there any new developments or trends in existing and potential ICT threats which the OEWG should discuss in-depth? In terms of new developments, we are currently implementing AI rapidly in 2024, be it Microsoft's 365 Copilot solution, or Read.ai which integrates with both Microsoft 365 and Google Workspace. During these implementations, the most important questions that CIOs and CISOs are facing around governance as it relates to security policies such as conditional access within these organizations because of the usage within AI.

What are specific ways in which states can further strengthen cooperation to ensure the integrity of the supply chain and prevent the use of harmful hidden functions? Are there existing programs/policies that help promote the adoption of good practices by suppliers and vendors of ICT equipment and systems?

SafePC Solutions is currently researching and writing a Whitepaper on ***"How to Identify Risks in Your Supply Chain Hardware and Software?*** *"*, In this whitepaper we discuss how to use a systematic process to identify risks.

To identify risks in your supply chain hardware and software, you should follow a systematic process that involves the following key elements:

- **Mapping your supply chain comprehensively,** identifying all the actors, processes, and assets involved in the production, distribution, and maintenance of your hardware and software components.
- **Assessing the threat landscape** and the vulnerabilities of your supply chain actors, processes, and assets to several types of risks, such as cyberattacks, sabotage, theft, fraud, corruption, natural hazards, etc.
- **Evaluating the impact and likelihood of each risk scenario** on your business objectives, such as customer satisfaction, operational efficiency, profitability, reputation, etc.
- **Prioritizing the most critical risks and developing mitigation strategies** to reduce their impact and likelihood, such as implementing security controls, diversifying suppliers, enhancing quality assurance, establishing contingency plans, etc.
- **Monitoring and reviewing the effectiveness** of your risk management process and updating it as needed to reflect changes in your supply chain environment.

I would like to reiterate your suggestion that we need to collaborate with other stakeholders and produce a working paper on the developing IT Security risks, and how supply chain within the ICT can assist with risk mitigation, and possibly conduct a workshop to build a toolkit for UN member states. We already started to partner with Write Pilot to give us a perspective on member states from the Middle East.