Telecommunications Industry Association
1201 Wilson Boulevard, Floor 27
Arlington, VA 22209 | www.tiaonline.org

My name is David Stehlin, the CEO of the Telecommunications Industry Association (TIA). I appreciate the opportunity to speak to this Subcommittee about this extremely important subject: securing the Information Communications Technology (ICT) supply chain so Americans can depend on trusted, secure, resilient, high-speed networks.

I have been CEO of TIA for the past 5 years and have run both publicly traded and venture backed telecom technology companies over my 40 years in the industry. I've seen tremendous change and technology improvements and have learned that security improvements always lag technology advancements. I've experienced, firsthand, how state-owned entities like Huawei operate on the global stage, undermining a competitive market of trusted ICT vendors.
As a graduate of the U.S. Naval Academy and a former Marine officer, I take the national security threat posed by entities controlled by our adversaries seriously, especially in light of the ever growing critical role of communications networks.

For more than 85 years, TIA has, with our 400 member companies, developed technical and process improvement standards and advanced new technologies that drive our economy. TIA's current standards cover a wide range of areas, including cell tower structures, data center infrastructure, structured cabling, public safety radios, hearing aid compatibility with mobile devices, telecom quality management and our most recent focus on supply chain security.
We are technology-agnostic, meaning that we support wireline, wireless and satellite technologies. In short, TIA has nearly a century of experience in ensuring that communications networks are built efficiently and resiliently with trusted suppliers.

The complexity of our networks as well as the reach of networks has grown dramatically in the past decade and we should anticipate that the number of connected IoT devices, for example, will reach over 30 billion in just the next five years.

Attacks come from many directions including, state sponsored enemies, criminals, and terrorists. While the attack possibilities are endless, we must have a defense in depth which starts with supply chain security. Ensuring that the products and services that make up our networks are coming from trusted suppliers who can demonstrate that security is designed into their products.

And we should remember that security is a sub-set of quality, a high quality product must be a secure product.

The US Government recognizes that supply chain vulnerabilities are forecasted to be a top network attack vector. Just last week, the Cybersecurity and Infrastructure Security Agency released a joint Cybersecurity Advisory with other U.S. agencies and trusted governments, focused on common vulnerabilities exploited in the supply chain.[1] These vulnerabilities are being exploited at an increased rate and the report found that many of these risks would have been mitigated by implanting a secure-by-design approach to ICT products and services.

[1] Cybersecurity Advisory, *2023 Top Routinely Exploited Vulnerabilities,* Cybersecurity & Infrastructure Security Agency (Nov. 12, 2024) (*available at* https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-317a).

The industry recognizes this and that is the reason we at TIA initiated and developed SCS 9001, the ICT industry's first Supply Chain Security standard in 2022. This standard was designed with input from both U.S. and trusted allied governments and aligns with and operationalizes the NIST Cybersecurity Framework, the Prague Principles, and many other guidelines.

SCS 9001 is a supply chain security management system intended to define and measure the requirements and controls for design, development, production, operations, and service of ICT products and services. By aligning with the standard, suppliers can demonstrate and verify that their products and services can be trusted.[2]

As network architectures continue to advance and become more complex, the potential attack surface grows and expands as well. This gives bad actors, including those which are state-sponsored from foreign adversaries, more targets. The need for security is further illustrated by the unique role communications networks play in our infrastructure – Every one of CISA's 16 identified critical infrastructure networks is fundamentally driven by ICT networks.

I believe these many past high-profile attacks, such as the recent Salt Typhoon attack, clearly indicates the need to address vulnerabilities within our ICT supply chain and mitigate them wherever possible.

A public-private partnership that builds in the elements needed to verify trust and continually improve, can change behavior and reduce the effect that bad actors have on our critical networks.

Thank you for your time today. I am happy to answer any questions you might have.

David Stehlin
Chief Executive Officer
Telecommunications Industry Association

[2] For instance, TIA has reviewed the vulnerabilities exploited in the high-profile Log4j breach and determined that SCS 9001 certification would have mitigated the vulnerability and limited exposure. A detailed summary of this review is available here: https://tiaonline.org/wp-content/uploads/2022/07/Log4j-vs-SCS-9001.pdf