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

Executive Summary

David Stehlin, CEO of the Telecommunications Industry Association (TIA), will testify before the subcommittee on the importance of securing the future of telecommunications infrastructure. He will emphasize TIA's long history of developing standards and advancing technologies to improve the lives of citizens and drive the economy. Stehlin will highlight the growing complexity and reach of networks, particularly with the rise of connected IoT devices and cloud-based data centers. He will stress the need for supply chain security to ensure that products and services come from trusted suppliers, and the importance of building high-quality networks with security and resiliency in mind. Additionally, Stehlin will address the growing concern over subsea cable systems, which carry the majority of internet traffic and financial transactions across continents, and the challenges posed by nefarious actors disrupting these cables. He will discuss the threat from untrusted software, hardware, and suppliers, and the need for a public-private partnership to verify trust and continually improve network security. Stehlin will conclude by highlighting TIA's efforts to develop the SCS 9001 supply chain security standard and the importance of working with allied countries to build secure, global networks.

Written Testimony

Chairman Hudson, Vice Chairman Allen, Ranking Member Matsui, and members of the subcommittee - My name is David Stehlin, the CEO of the Telecommunications Industry Association (TIA). I appreciate the opportunity to speak to this Subcommittee about this important subject: Securing the Future of the Telecommunications Infrastructure, so that Americans can depend on trusted, secure, resilient, high-speed networks.

For more than 85 years, TIA has, with our 400 member organizations, developed technical and process improvement standards and advanced new technologies that drive our economy and improve the lives of our citizens. TIA’s current standards cover a wide range of areas, including Data center infrastructure, cell tower structures, structured cabling, public safety/ emergency responder radios, hearing aid compatibility with mobile devices, telecom quality management and our most recent focus on cyber and supply chain security.

We are technology-agnostic, meaning that we support all wireline, wireless and satellite trusted technologies. In short, TIA has nearly a century of experience in ensuring that communications networks are built efficiently and resiliently with trusted suppliers.

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, but I also recognize that security improvements always lag behind 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.

The complexity and reach of networks have grown dramatically in the past decade, and that growth is accelerating. For example, the number of connected IoT devices in our homes already numbers in the billions, and will reach over 30 billion in just the next five years. Most networks today are cloud-based which means that data centers are at their hub. And these data centers rely more and more on Artificial Intelligence and the Graphics Processing Units (GPUs) which are vital to power these AI applications. Keeping these data centers secure as our intent is to keep the U.S. safe and forward-leaning while we live in a globally connected world. If we want our tree of prosperity to flourish, we need to ensure all the connected roots are healthy.

Every type of critical infrastructure: from the electric grid to water systems, to emergency responders, to the internet that we use to communicate and conduct business, all use similar information communications technologies and systems. Potential vulnerabilities in these

systems have a broad impact due to the unique role played by communications networks in our infrastructure. Every one of CISA's 16 identified critical infrastructure networks is fundamentally driven by ICT networks.

Network 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. We must ensure that the products and services that make up our networks are coming from trusted suppliers who can demonstrate that security is designed in.

We must verify before trusting. And we should remember that security is a subset of quality, a high-quality network must be based on infrastructure built with security and resiliency in mind. All of this is critical to the success of building trusted, resilient, and secure global networks.

In this context, subsea cable systems are an area of growing concern. From the Red Sea to the Taiwan Strait, to the Baltic Sea and beyond, nefarious actors are increasingly disrupting global networks by cutting cables and damaging the points where the cables come ashore. These subsea cables carry 99% of internet traffic across continents, and more than $10 trillion of financial transactions. These cables are the irreplaceable backbone of the global internet, and while satellite communications play an integral role in our networks, the data capacities of subsea cables cannot be overstated. For instance, we have seen estimates that by 2026, the total

global satellite capacity is expected to be about half a percentage of the total global subsea cable capacity.[1]

Despite the essential nature of this technology, cables are increasingly getting caught up in an endless cycle of red tape. Well-intentioned efforts by the DOJ-led interagency group known as Team Telecom to mitigate national security threats have made laying new cables increasingly difficult. This has had the practical effect of reducing cable redundancy, which makes U.S. subsea infrastructure more susceptible to cuts or breaks. We must take the necessary steps to ensure that the U.S. remains at the forefront of promoting common-sense practices for subsea cable deployment that appropriately balance the critical national security roles this infrastructure plays with the economic realities of cable deployment.

Of course, in addition to these physical threats to our communications networks is the fundamental threat from untrusted software, hardware and suppliers. 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 that are state-sponsored by foreign adversaries, like the Chinese Communist Party, more targets. For example, the recent Salt Typhoon attack.

The US Government has a long and bipartisan recognition of the threat supply chain vulnerabilities pose to our nation's infrastructure, and there is a shared consensus that these vulnerabilities are forecasted to be a top network attack vector. 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 our members and

[1] Dan Swinhoe, *Space Comes for Fiber: Can Satellites Offer Data Centers a New Resiliency Option?*, Data Center Dynamics (Sept. 29, 2023), https://www.datacenterdynamics.com/en/analysis/space-comes-for-fiber-can-satellites-offer-data-centers-a-new-resiliency-option/

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 the 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]

This is an effort that reaches beyond our domestic infrastructure, and TIA has been working with the Departments of Commerce and State as they help allied countries build trusted networks. As I previously mentioned, in a connected world, it is critical that our partners also build security into their wireless, wireline, satellite and critical infrastructures.

I believe these many past high-profile attacks, such as the previously mentioned Salt Typhoon attack, clearly indicate the need to address vulnerabilities within our ICT supply chain and mitigate them wherever possible. Before Salt Typhoon was the hacking of U.S. presidential campaigns, the CrowdStrike vulnerability, the SolarWinds hack, and many others that we must not forget. The growing number and sophistication of these attacks should concern us all.

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 many critical networks.

[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

We appreciate the leadership that this committee has demonstrated by holding this hearing today, and I would like to thank you for your time. I am happy to answer any questions you might have.

David Stehlin
Chief Executive Officer
Telecommunications Industry Association