Telecommunications Industry Association

TIA Position Paper

SECURING THE NETWORK AND SUPPLY CHAIN WITH INDUSTRY-DRIVEN STANDARDS

JANUARY 2020

Trust in ICT Supply Chain Security Can Only Come from Global Industry-Driven Standards and Programs

The global telecommunications infrastructure and the information and communication technology (ICT) supply chain are at a greater risk than ever before. The ICT industry has an obligation to ensure that the devices, equipment, and networks global businesses and consumers rely on can be trusted. We need to be doing all we can to minimize exposure to cyberattacks that threaten to endanger national security, disrupt critical infrastructure, and impede economic growth.

New wireless, IoT, 5G, and compute-rich networks and technologies are being deployed to support advancements like self-driving vehicles, fully automated smart buildings, and artificial intelligence (AI). Trust is the foundational principle for technology adoption, and those involved in developing and deploying emerging technologies and the infrastructures that support them must earn that trust through demonstrated and transparent accountability and verification that can only come from global, industry-driven standards and programs.

A NEW LANDSCAPE OF RISK

Over the past decade, the fragmentation of the ICT supply chain has resulted in a growing number of suppliers, manufacturers and service providers developing and deploying the hardware and software that comprise the world's telecommunications infrastructure. This shift has enabled the globalization of ICT resources and is driving networks to become more software driven and reliant on white-box equipment and open-source software that gives users more choices and flexibility.

The Complex Network is More Vulnerable than Ever

With this new network landscape, the ICT supply chain has become increasingly complex and vulnerable at any point along its lifecycle. With more equipment, connected devices and global players than ever, security risk is at an all-time high. Threats are continuing to evolve as criminals and bad-actor nations now have more ways to develop sophisticated cyberattack techniques and back-door mechanisms that cause harm, including:

- **Malicious data breaches** that provide unauthorized access to business financials, intellectual property, consumer data, and other sensitive information
- **Denial-of-service (DoS) attacks** that disrupt critical infrastructure and disable operations
- **Counterfeit components** that unintentionally or deliberately impact reliability and increase exposure to additional back-door mechanisms and malware

GLOBAL AND ECONOMIC IMPACT

As a result of increased threat vectors within the ICT supply chain, developed nations around the world, including the U.S., Canada, Australia, Japan, and much of Europe are enacting legislation and government regulations addressing cybersecurity. In November 2018, the U.S. signed into law the Cybersecurity and Infrastructure Security Agency Act, the FCC has adopted regulations that ban recipients of U.S. government funds from using untrusted vendors, and the Department of Commerce has released rules prohibiting potentially risky private sector transactions with foreign adversaries. Similar initiatives are happening around the world.

Business Continuity and Consumer Trust are Critical for our Economy

Government action is a necessary and important aspect of ICT supply chain security, especially to protect classified information and prevent the take-down of critical infrastructure. While these threats are at the pinnacle of governments' security concerns, the global and economic impact of ICT supply chain security are much further reaching.

- **Business continuity** – With all aspects of business now relying on the transmission of information and communication across networks, disruption within any element of the supply chain can bring businesses to a halt, leading to lost revenue, reduced profits, and an inability to meet customer demand.
- **Corporate reputation** – Supply chain disruptions and cyberattacks can create long-term damage to a company's reputation. Whether it's a delay in getting new products to market or something more serious like the theft of business financials, intellectual property or consumer information, unmanaged supply chain risk can impact consumers' willingness to purchase products, or to recommend or work for a company.
- **Consumer confidence** – Whether it originates from a single known company falling victim to a security breach, or a wide-spread infrastructure failure, a lack of consumer confidence impacts the entire industry and slows the acceptance of new technologies. For example, consider a technology like self-driving vehicles that will rely on low-latency, high-bandwidth 5G networks. As the technology advances, any

risk to the underlying infrastructure – from 5G network communication and curbside traffic detection systems, to the vehicular sensors and autonomous control software – can destroy consumer confidence in the technology and prevent adoption altogether, hindering innovation and economic growth.

- **Interoperability** – Facilitated by open industry standards, the ICT industry as we know it today is founded on every component within the network, regardless of vendor, working seamlessly together to effectively transmit information. Interoperability is critical to driving continuous innovation and ensuring consumer choice, ease of use, and competition. Any maliciously tainted or counterfeit products entering the supply chain threatens to destabilize the open concept and hinder interoperability.

Industry-Driven Standards will Build Needed Trust

Ensuring the trust and integrity of the ICT supply chain requires accountability and verification that can only come from industry-driven standards, measurements, and benchmarking that form a consistent, common, and accepted set of global requirements. There is no one with the industry experience, know-how, affiliations, advocacy, and influence who is more prepared and qualified to lead the way on ICT supply chain security than the Telecommunications Industry Association (TIA).

WHY INDUSTRY-DRIVEN STANDARDS AND ASSESSMENTS?

While government policies are a necessary and important aspect of ICT supply chain security, especially when it comes to preventing risks to national security and public health or safety, federal regulations alone cannot provide the level of detail required to address all aspects of the ICT supply chain and keep up with the constantly-evolving and broad-reaching technology landscape.

Government Regulations Alone are Inefficient and Increase Costs

Relying solely on government policy to address ICT supply chain security can present the following consequences that can adversely impact the economy:

- **Bureaucracy and inefficiency** due to the inherent nature of slower government approvals and decision-making processes coupled with influence from special interest groups that can hinder finalizing or issuing regulation and legislation.

- **Unnecessary trade restrictions and regulations** due to broad-reaching government policy that does not address the specific needs of businesses involved in the ICT supply chain.

- **Decreased competition, higher prices, and reduced profit** due to reactive regulatory mandates that create high costs to comply for existing businesses and deter the startup of new business, which increases prices for consumers and decreases competition.

- **Stifled innovation and investment** due to costly regulations and complex requirements that force businesses to channel their talent into dealing with lengthy compliance processes rather than investing in new technologies.

Industry-Driven Standards Foster Innovation and Investment

In contrast, proactive and preemptive industry-driven standards and programs are created via consensus by expert individuals and companies entrenched in the development and deployment of global ICT products and services. When developed by the very industry players whose livelihood is affected by ICT supply chain security, the measurements and benchmarking behind these standards and programs can offer a more systematic, repeatable framework that is tailored to address specific product and service categories without hindering competition, innovation, and investment.

Moreover, decision-making in industry-driven standards and programs is not delayed by slow government processes and bureaucracy, making them timely and quick to respond to industry issues. Industry standards-making bodies also have procedures in place to maintain transparency and continually monitor and improve standards and programs to adjust to evolving markets and technologies, which drives continual improvement and incents investment.

That's not to say that local, state, and federal governments don't have a role. The public and private sectors must come together to tackle ICT supply chain security quickly and efficiently, and in a way that addresses the specific needs of all interested parties and encourages economic growth.

WHY TIA, WHY NOW?

While other industries like food, drug, and aviation have taken measures to improve security and safety, the need for global industry-driven ICT supply chain security standards and programs is overdue. Low-latency networking, 5G, sensor technologies, and IoT are happening now and paving the way for technological advancements. Without ICT supply chain security standards and programs that give companies, the government, and consumers alike the confidence that our vast, complex telecommunications network can be trusted to be reliable and secure, investment into and adoption of new technologies will come to a screeching halt.

TIA has the Experience and Capability to Lead

The ICT industry must immediately lead the way on supply chain security, and TIA is prepared and qualified to lead through its four communities of technology, government affairs, standards, and business performance.

- **TIA represents more than 400 companies and involves 2,500 key players and thought leaders representing all aspects of the ICT supply chain** and is leading the way to successfully launch new and emerging technologies like vehicular telematics, smart buildings, smart device communications, smart utility mesh networks, and edge data centers.

- With strong government alliances and in-depth analysis of pending regulations and legislation, **TIA has the unique ability to engage with bipartisan domestic and international policymakers** and bestow instrumental influence to advocate for policies that address supply chain security, while encouraging innovation and investment in network infrastructure.

- **TIA, together with its members, has developed more than 3,600 telecommunications industry standards** and continually improves those that are relevant to the ICT industry, covering a broad range of technologies, including private radio equipment, cellular towers, structured cabling, satellites, and smart device communications.

- **TIA provides resources, strategic guidance, and business intelligence to the ICT industry** by driving scalable, repeatable, consistent processes, and programs that bring tangible value to ICT companies to enhance their bottom line.

TIA also has the track record and experience to take the lead globally on ICT supply chain security. Domestically, TIA's government affairs team is leading advocacy efforts on ICT supply chain security, working with U.S. government entities to establish a set of "trust principles" as the first step in safeguarding telecom infrastructure and actively participating on the Department of Homeland Security's ICT Supply Chain Risk Management Task Force. Abroad, TIA works with telecommunications regulators across Europe and Asia as these governments attempt to establish their own approaches to securing critical infrastructure and networks. In 2019, TIA signed a memorandum of understanding (MOU) with Indian telecommunications regulators to enhance cooperation on 5G deployment. As a founding member of the Beijing-based United States Information and Technology Office (USITO), TIA has worked to ensure that China's approach to cybersecurity is inclusive of global companies with proven networks solutions.

The QuEST Forum TL 9000 Quality Management System, part of TIA's Business Performance Community, has been successfully meeting supply chain quality requirements of the worldwide ICT industry for more than 20 years. TL 9000 specifically helps companies meet the supply chain quality requirements of the global communications industry through effective third-party performance-based measurements, assessments, benchmarking, and reporting. With TL 9000, TIA has the experience and a successful foundation in place to adapt and/or build upon this established common set of supply chain quality requirements to address security.

WHO WILL BENEFIT?

Standards and programs driven by TIA can measure, assess, and benchmark the integrity of telecom devices, components, networks, and services – and the companies that deliver them – thereby continually raising the bar on ICT supply chain security, while lessening the need for government intervention and delivering significant benefits to all players and their customers.

Industry, Consumers and Governments will Benefit from Trusted Standards

- **Manufacturers, buyers and suppliers** will benefit from the validation of the devices and components that they produce, purchase and supply via analysis against security benchmarks and third-party objective evaluations, reducing the cost of audits and compliance with unnecessary trade restrictions and regulations that can lead to increased prices, decreased competition, and stifled innovation and investment. Transparent reporting will also help maintain interoperability, while substantiating the corporate reputations, business practices, and country of origin of original equipment manufacturers (OEMs) and raw material suppliers via set expectations and requirements.

- **Service providers, system integrators, and contractors** involved in the deployment of systems and infrastructure or the transmission, collection, processing and storage of information can drive consumer confidence by ensuring the protection of data through audited security measures and the deployment of components, products and systems from verified and trusted suppliers that have met the standards. As a result, supplier relationships are improved across the entire ICT supply chain.

- **Organizations and their executives across all vertical markets** can have confidence that their internal and external networks have built-in versus bolted-on security by utilizing components and services from trusted companies that have been thoroughly vetted by adhering to industry-driven standards and programs. This enables these organizations to ensure business continuity, faster time to market, and a competitive advantage.

- **State, local, and federal governments** can rest assured that the products and services required for the deployment of new networks and technologies have been assessed for risk through standards and programs designed specifically for these complex systems, allowing them to focus their attention on threats that have a direct impact on national security and public health and safety.

WHAT'S NEXT?

Creating comprehensive industry-driven supply chain security standards and programs to verify the safety and security of all ICT infrastructure devices components and build trust in the vast and complicated network of ICT supply chains will require significant effort, but it has been done before. Through TIA, the ICT industry already has standards and model programs in place that can quickly adapt to address the challenge.

TIA has Initiated a Task Force that will Work to Develop Standards

The development of ICT supply chain security standards and programs are perfectly aligned with TIA's existing capabilities and will drive corporate, government and consumer confidence that our vast telecommunications networks are secure. To that end, TIA is actively executing domestic and global policy-related advocacy programs and through its QuEST Forum arm has initiated the formation of an industry-led task force and committees to begin developing standards and assessment programs for ICT supply chain security that will:

- **Define requirements** and provide a consistent, common, and mutually understood set of security expectations through ongoing comprehensive measurement and benchmarking of the integrity of devices, components, and companies involved across all aspects of the global ICT supply chain. And these requirements will be continually and pro-actively updated as technology advances to stay ahead of potential risks rather than responding to issues after they arise.

- **Provide transparent, comprehensive reporting** that identifies trusted manufacturers, buyers, suppliers, service providers, integrators, and contractors, while allowing these companies to monitor, track, and continually improve the integrity of their products and services and raise the bar on security as technology advances.
- **Eliminate the need for multiple security standards and unnecessary government regulations** and intervention, thereby reducing the cost of doing business and enabling ongoing innovation and investment in new products and technologies.

Ready to join TIA in the development of these standards and programs to address the growing concern of ICT supply chain security?

Learn more at: supplychainsecurity@tiaonline.org or www.TIAonline.org