

TIA SUPPLY CHAIN SECURITY PROGRAM



The First ICT-Specific Standard for Supply Chain Security

The cyber terrorism threat has never been higher and is now expected to inflict a cost to organizations and countries of over USD \$10 trillion per year. Attacks directed at the information communications technology (ICT) supply chain level are especially strategic for foreign adversaries and present the utmost concern as they have the potential to impact widespread global networks. Furthermore, the widespread adoption of new applications leveraging Internet of Things (IoT) devices, that require internet connectivity, create more entry points for cyberattacks causing enormous risk to consumers, businesses, and governments. However, existing standards that address cybersecurity across various industries have historically not focused on the supply chains behind the networks that connect them.

This is a critical time for the ICT industry to act. Key players and thought leaders involved in developing and deploying solutions that comprise the world's digital communications infrastructure must ensure the trust and integrity of the ICT and IoT supply chains. TIA is leading the way and since 2022, TIA's SCS 9001 Cybersecurity and Supply Chain Standard has provided an industry-driven, process-based methodology to address the critical, urgent need for ICT supply chain security. Certification to the standard allows network operators, service providers, system integrators, manufacturers, buyers, and suppliers across the global ICT supply chain to demonstrate that the software, hardware, and other ICT components they produce, purchase, and deploy meet critical security benchmarks to mitigate the risk of cybersecurity attacks. Future releases will address improved support for government requirements, increased coverage for cloud-based services and enhancement to cover IoT supply chain security.

TIA IS LEADING THE WAY

The Trusted Industry Association for the Connected World

As both a standards and trade association, TIA is uniquely qualified to address ICT supply chain security. With over 400 members from around the world, including manufacturers, service providers, consultants, and more, TIA has addressed many industry-wide challenges in the past such as creating the global ICT quality management system, TL 9000, and the dominant technical standards for data centers and wireless towers.

TIA's QuEST Forum has an active working group of engineering and security experts with various subcommittees assembled to define, publish, and enhance the SCS 9001 standard. The SCS Workgroup has outlined a roadmap for this new standard and certification program that includes coverage for emerging technologies broadening the reach of connectivity such as low-latency networking, 5G, advanced Wi-Fi, sensors, and IoT/IIoT implementations. As an industry, we must ensure that security measures and controls can evolve alongside technological advancements.

A Foundation of Trust and Continual Improvement

Security is a critical aspect of quality—products and services cannot be considered for acceptable levels of quality without also being secure. To that end, the SCS 9001 standard incorporates a process-based architecture that is a systematic, repeatable framework and uses measurements and benchmarking as a vehicle for driving continual improvement.

As the first ICT-specific standard for global supply chain security, SCS 9001 ensures trust can be verified via the following unique features:

- Integrates selected ICT-related requirements and controls from existing recognized standards and eliminates gaps via additional ICT supply chain security process requirements.
- Employs security performance measurements for certification that are then aggregated to provide anonymous industry benchmarks for continual improvement.
- Incorporates structured 3 factor risk assessment, secure software development life cycle best practices, protection against counterfeiting, and use of software bill of material (SBOM).
- Converts and augments relevant supply chain security controls (selectively applied) to general process requirements (generally applied) to assure assets are protected.
- Incorporates non-technical principles of trust to assure that suppliers are transparent relative to international government/regulatory body requirements and policies.
- Organizations are audited by Multilateral Recognition Arrangement-accredited third-party Certification Bodies whose auditors must meet specific competency requirements.

Advocating for the Industry

Government policies are a necessary and important aspect of ICT supply chain security. However, federal regulations alone cannot provide the level of detail required to address all aspects of securing the ICT supply chain and keep up with the constantly evolving and broad-reaching technology landscape. TIA's government affairs team is playing a critical role by leading advocacy efforts on ICT and IoT supply chain security, actively engaging with domestic and international policymakers to advocate on policies for supply chain security.

GET INVOLVED

To adequately create a measurable and verifiable standard that meets the needs of all stakeholders, we need to have those stakeholders involved in developing and deploying SCS 9001. As the trusted association for the connected world, TIA provides the neutral ground for stakeholders across multiple verticals, company types and industries to come together to:

- Establish a set of security requirements through comprehensive third-party assessments, measurements, and benchmarking.
- Continuous enhancement of the standard to address new technologies, applications and industries leveraging ICT infrastructure.
- Provide transparent, comprehensive reporting of SCS 9001 certified ICT manufacturers, suppliers, service providers, integrators, and contractors.
- Eliminate existing gaps by developing new industry-driven standards to ensure the security of devices, equipment and networks that comprise the ICT supply chain.

The stakeholders include, but are not limited to, professional experts from: IOT business enterprises, equipment manufacturers, government agencies, service providers, integration service providers and consultants.

If you are interested in joining our working group and securing the global ICT and/or IoT supply chains, please contact us at supplychainsecurity@tiaonline.org

Learn more at: <https://tiaonline.org/what-we-do/technology-programs/supply-chain-security/>.