TIA

WHITE PAPER

SCS 9001: THE FIRST ICT-SPECIFIC STANDARD FOR GLOBAL SUPPLY CHAIN SECURITY

New Measurable Standard From TIA Will Ensure Trust Can Be Verified

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The information and communications technology (ICT) industry has an obligation to ensure that the devices, equipment, and networks relied on by businesses and consumers, can be trusted. The threat to the global communications infrastructure and the ICT supply chain has reached an all-time high. Emerging technologies will further expand the attack surface. While existing standards address cybersecurity across various industries, historically they have not focused on the ICT supply chain. Supply chain attacks in this industry have the potential to impact global networks and tens of millions of users.

The Telecommunications Industry Association (TIA) believes that security is a subset of quality given one cannot have a quality product or service if it cannot be trusted. As such, ensuring the trust and integrity of the ICT supply chain using standards requires a criteria that can evolve alongside the technology and not fall behind the rate of technological advancement. This is accomplished by using a quality management system (QMS) process as the basis for producing a measurable and verifiable standard. TIA is leading the way on ICT supply chain security with the development of the first-ever global SCS 9001 standard that specifies verifiable and measurable criteria and uses a process-based QMS to verify trusted suppliers.

To date, TIA has managed the development of more than 3,600 ICT industry technical standards created by our member companies and their volunteers. In addition, through its QuEST Forum business performance improvement community, TIA built and maintained the ICT industry's process-based quality management system for over 20 years. Based on this combined experience, TIA's Supply Chain Security (SCS) Workgroup, comprised of equipment providers, service providers, and security experts, has been developing the SCS 9001 supply chain security standard at an accelerated pace since early 2020. Based on ISO 9001 and TIA's TL 9000 standard, SCS 9001 will incorporate relevant requirements and controls from existing standards, address gaps specific to securing the ICT supply chain, and include additional supply chain process requirements. The SCS Workgroup identified all ICT assets to be protected, determined top-level requirements, and outlined a roadmap for the release of the SCS 9001 standard and certification program later this year. Nine SCS Workgroup teams have been drafting key requirements for the standard, while also informing and consulting various government agencies.

The SCS 9001 standard will provide the means for service providers and manufacturers to demonstrate and ensure that their supply chains meet the critical benchmarks needed to mitigate risk of cybersecurity attacks. This will ultimately increase trust in the ICT supply chain, while preventing exposure to cyberattacks that threaten to endanger national security, disrupt critical infrastructure, and impede economic growth.

Please join us in this critical and unprecedented effort.

INTRODUCTION

Global cybercrime and cyber terrorism is expected to cost more than USD $6 trillion in 2021 alone.[1] While global economies are increasingly dependent on communications infrastructure and the technology it connects, the cyber terrorism threat has never been higher. Recent threats and failures have sparked a new realization of urgency among federal government agencies, utility companies, service providers, equipment manufacturers and ICT leaders alike.

The increasingly complex and vulnerable ICT supply chain and the rise of cyberattacks by sophisticated criminals and foreign adversaries threaten to endanger national security, disrupt business continuity, and devastate consumer confidence—all with vast economic consequences. To address this critical issue, TIA members launched a new initiative in early 2020 to build a much-needed industry-driven ICT supply chain security standard and program. As a leading industry association and standards development organization, with the track record and experience to reinforce the integrity of the ICT supply chain, TIA leveraged its QuEST Forum arm of industry-led working groups and security experts to develop the industry's first global, industry-driven supply chain security standard. Over the past year, TIA's embodied Supply Chain Security (SCS) Workgroup has been diligently executing this initiative, with the landscape analysis complete and standards development well underway.

The result of this assiduous work is the upcoming release of the SCS 9001 standard that specifies the criteria for a process-based QMS that builds upon the best of existing industry and government-recognized standards and adds ICT-specific requirements to ensure all aspects of supply chain security are addressed. Through clearly defined measurements that can be audited and verified, this essential new standard will allow ICT manufacturers, suppliers, and service providers to benchmark themselves against the requirements and demonstrate supply chain security compliance through an accredited certification process. SCS 9001-certified organizations will ultimately build stakeholder confidence and help ensure trusted devices, equipment, and networks across the entire ICT supply chain to prevent exposure to devastating cyberattacks that are threatening our world.

AN URGENT PRIORITY

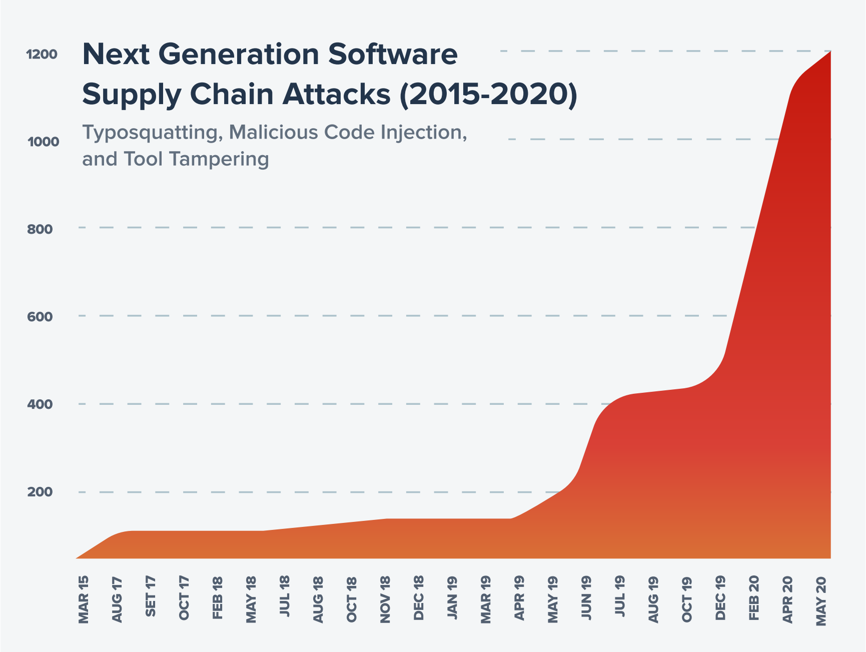
The introduction of new technologies and fragmentation of the ICT supply chain has enabled the globalization of ICT resources and precipitated networks to become more software driven. While this shift gives users more choices and greater access to feature-rich applications and technologies via faster development, it also extends the ICT supply chain and makes it more complex and vulnerable.

SOFTWARE DEVELOPMENT AND QUALITY IS ESSENTIAL

As networks, solutions, and products become more software driven and require thousands or even millions of lines of code upon which an increasing number of applications are built, ensuring that developers are trusted, and their output is verified is critical to securing the ICT supply chain. Additionally, free and open-source software code can be accessed by all users, and with **studies showing that effectively all (99%) codebases audited in 2020 contain at least one open-source component, there is a greater risk for gaps in poorly-written or under-managed code that makes software susceptible to attack.**[2] As companies integrate more pre-built, open-source code from third parties into their ICT equipment, devices, systems, and applications, the potential for malicious back-door mechanisms to infiltrate entire networks is further increased.

The trend of relying on cloud-based technologies and outsourcing IT to managed service providers (MSPs) as consumers and businesses strive to keep pace with the digital economy can be both a way to mitigate risk and a vector for attack on a network. A growing number of MSPs around the world are being targeted by hackers as they can serve as launchpads into multiple corporate networks. To top it off, the increased use of cloud-based services for remote digital access fueled by the Covid-19 pandemic has equipped attackers with even more points of entry. **Since the onset of the pandemic, the U.S. FBI reported a 300% increase in reported cybercrimes.**[3]

In early February of this year, a Florida water treatment plant was targeted via cloud-based remote-access software used to allow staff to remotely troubleshoot IT issues, enabling an intruder to temporarily command an increase in sodium hydroxide to deadly levels in the water supply—an attack that that was thankfully thwarted due to other security and monitoring measures in place.[4] According to one recent report, next-generation (i.e., upstream open- source) **software supply chain attacks surged 430% over the past five years**, with an evident and significant jump coinciding with the onset of the pandemic.[5]


Next Generation Software Supply Chain Attacks (2015-2020)

Typosquatting, Malicious Code Injection, and Tool Tampering

ICT SUPPLY CHAIN ATTACKS ARE OF THE UTMOST CONCERN

While internal cybersecurity practices like encryption, firewalls, and other practices are critical for organizations to protect their internal networks, the reality is that virtually all networks are comprised of equipment, devices, and software from outside suppliers that make up the complex and global ICT supply chain. Compromised components can be difficult to detect if they are functioning as expected, yet these components are also made up of multiple sub-components from multiple suppliers and locations around the globe—everything from memory chips, processors, and motherboards, to hard drives and graphic cards.

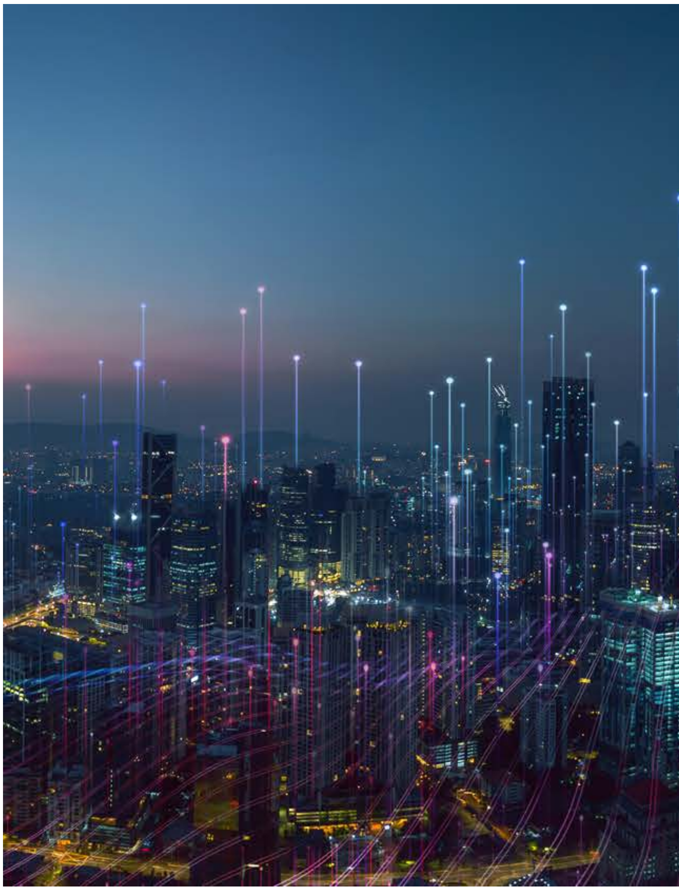
Many of these ICT-related components and sub-components have reached commodity status and are increasingly purchased from low-cost and potentially compromised suppliers that may have been undermined by organized crime or by foreign adversaries. Add to these components millions of lines of software code from third-party sources and shorter product life cycles—combined with the fact that these components are deployed globally and accessed by millions of users—it is clear to see why supply chain security is of the utmost concern.

Cybersecurity attacks achieved through hardware and software deep within the supply chain have the potential to quickly escalate and distribute downstream across tens of thousands of networks and millions of users. This level of attack does not just bring a business to a halt, damage a corporate reputation, and sow consumer distrust in technology—it also has the potential to destabilize the entire ICT industry, hindering interoperability and continuous innovation. A particularly massive assault with a direct supply-chain element, especially from foreign adversaries, has the capacity to severely damage an entire national economy, disable critical infrastructure, and significantly weaken public safety services.

ICT SUPPLY CHAIN ATTACKS ARE OF THE UTMOST CONCERN

Supply-chain attacks have been steadily on the rise over the past decade, with 2017 seemingly a watershed moment with at least seven major attacks.[6] Disasters like the Equifax supply-chain data breach affecting 143 million consumers stemmed from more than 30 backdoors into systems via application frameworks. Uber's massive data breach that same year happened when hackers accessed open-source code within a repository containing log-in credentials for other systems. A server misconfiguration at a large service provider resulted in the release of name, mobile number and account PIN for 14 million customers in 2017.

Attacking at the ICT supply chain level is especially strategic for foreign adversaries like Russia, Iran, and North Korea have proven to be hostile cyber actors seeking to fulfill a wide variety of geo-political and economic goals.



Consider the 2017 Russian-sponsored malware NotPetya that weakened Ukraine's power and transit infrastructure and central banking system in preparation for an invasion.[7] There was also the sophisticated software supply chain attack dubbed "Kingslayer" linked to the Chinese group Codoso that targeted an otherwise legitimate Windows administrator application to gain access to organizations' networks, with victims including 5 major defense contractors, 4 major service providers, 10 military organizations, and 24 financial institutions.[8]

In 2019, the Chinese-backed APT41 advanced persistent threat (APT) group was blamed for gaining access to ASUS equipment and delivering malware to millions of other ASUS computers manufactured in Taiwan by the world's sixth-largest computer vendor.[9] More recently, SolarWinds, a company that provides popular IT monitoring and management software, had malicious code inserted its Orion management platform. This product was then installed in nearly 18,000 enterprises, technology providers, and government agencies. The attack is believed to stem from Russian-backed hackers.[10] And in February 2021, researchers at Stanford University warned that the popular audio chat app Clubhouse may be leaking user metadata to the Chinese government through a Shanghai-based software company's back-end infrastructure.[11]

Unfortunately, amidst a global economy still fragile from the Covid-19 pandemic and political discord across multiple regions, these recent high-profile attacks are proving that the threat level within the ICT supply chain is at an all-time high and needs immediate resolution.

TECHNOLOGY IS OUTPACING SECURITY

While the threat is immediate and evident, new emerging technologies are advancing faster than security protocols and therefore have the potential to expand the attack surface, providing more entry points for malicious intent. Wireline deployments and mobile deployments, including 5G and beyond technologies not only introduce vulnerabilities by connecting tens of thousands of new IoT devices, services, and autonomous systems that are targets for attack, but the push towards newer open software-defined radio and networking techniques, also increases the potential vulnerabilities through more integrations, a broader supplier base, and additional sources of software. As these networks reach into buildings and connect to even more IoT devices, it is expected that the number of elements managed in a network will increase by an order of magnitude or greater. **A 2019 survey indicated that 94% of service providers and industry experts are concerned about the escalation of security risk with the advent of 5G networks** driving growth in traffic, devices, and mission critical IoT applications.[12]

Open network architectures, software-defined solutions and Network Functions Virtualization (NFV) within 5G and in backhaul networks deployed for flexibility, manageability, and scalability also bring new security concerns. The virtual equipment is offered by multiple vendors, integrates with a variety of legacy equipment, and may be outsourced to third parties whereby they do not reside in data centers directly owned by service providers, increasing the potential for security gaps. While the 5G Open Radio Access Network (ORAN) concept based on gray-box or white-box hardware and open-source software from different vendors in theory may enable more interoperability, this open ecosystem further broadens the attack surface with new exploitable unsecure or untested interfaces.[13]

Ultimately, as our connections become more software-driven, there is a need for anyone producing, purchasing, and deploying ICT equipment and devices to further understand and verify ICT equipment suppliers, their suppliers, and their suppliers' suppliers throughout the entire supply chain, as well as how that equipment connects to other systems. Ensuring the trust and integrity of the ICT supply chain requires accountability and verification, which can only come from an industry-driven standard that specifies consistent, common, and accepted criteria with measurements, benchmarking, and compliance verification.

TIA IS ACCELERATING PROGRESS

Following TIA's early 2020 initiative to address ICT supply chain security through a global, industry-driven supply chain security standard, TIA QuEST Forum's SCS Workgroup immediately began the process of reviewing existing standards to assess the landscape and begin development for an ICT-specific, process-based standard that would ultimately become SCS 9001.

With the increasing level of urgency rising and lack of an existing standard, the workgroup accelerated the development process through the diligence and commitment of the workgroup member companies and their volunteers' tireless efforts. These workgroup members represent the key players and stakeholders that touch all aspects of the ICT supply chain:

- Service Providers
- Systems Integrators
- Manufacturers
- Security Experts
- Procurement Leaders
- Software/Hardware Suppliers

At the same time, recognizing that a secure ICT supply chain must also meet the needs of national and international governments, TIA's Government Affairs team has continually interfaced with various U.S. and global government agencies, advisory committees, task groups, and policymakers throughout the process.

BUILDING ON THE FOUNDATION OF TRUST

It is TIA's position that security is a critical aspect of quality—given products and services cannot be considered for acceptable levels of quality without also being secure. To that end, the SCS Workgroup determined early on that the new SCS 9001 standard must incorporate a QMS as a foundational element and use measurements and benchmarking as a vehicle for driving continual improvement. While completely avoiding any security breach is unrealistic, a QMS enables a thorough analysis of what triggered an event and initiate any needed changes in the process to prevent future recurrence.

The SCS Workgroup identified ISO 9001, the most widely deployed and recognized QMS, as the foundation for the new SCS 9001 standard. It also serves as the foundation for several other industry sector QMS standards, including the TIA QuEST Forum TL 9000 QMS Standard for ICT supply chain quality. Any organization certified to ISO 9001, or to any sector standard that fully incorporates and does not contradict ISO 9001, will meet the foundational requirements for SCS 9001.

THE LANDSCAPE ANALYSIS: A CRITICAL FIRST STEP

In any standards development process, the critical first step is to understand existing industry standards to assess their adoption and value within the industry and identify a structural foundation. Each standard is then carefully analyzed to determine relevant aspects to adopt or to identify any gaps. This is accomplished by mapping the coverage of existing industry-recognized standards to the requirements of the new standard.

While industry standards often have areas that overlap, the purpose of this exercise from an ICT supply chain security perspective is to ensure that all viable ICT-related aspects of existing recognized standards are integrated into the new standard. The goal of the landscape analysis is an ICT-specific supply chain security standard that could also be applied across multiple industries—from transportation, industrial, and finance, to education, retail, and hospitality. The SCS Workgroup analyzed over 30 existing standards across multiple industries, including, but not limited to:

- ISO 9000 series of standards for quality management
- ISO 27001 series of information security standards
- TL 9000 standard for quality management in the ICT industry
- NIST cybersecurity framework and Federal Information Security Modernization Act (FISMA) metrics
- Cloud Security Alliance Cloud Control Matrix (CCM)
- Cybersecurity Maturity Model Certification (CMMC) for the U.S. defense industrial base
- AS9100 series of standards for quality management in the aviation, space, and defense industry
- ISO/TS 16949 standard for quality management in the automotive industry

Each standard was carefully analyzed for its relevancy with the objective of ensuring that the new SCS 9001 standard references or incorporates any requirements and controls that enhance ICT supply chain security. The SCS Workgroup consciously chose to exclude elements not related to ICT supply chain security, as well as any element requiring investment that outweighed outcome benefits. Leveraging the deep knowledge and experience of the industry subject matter experts, the SCS Workgroup next began the process of adding requirements to fill any critical gaps.

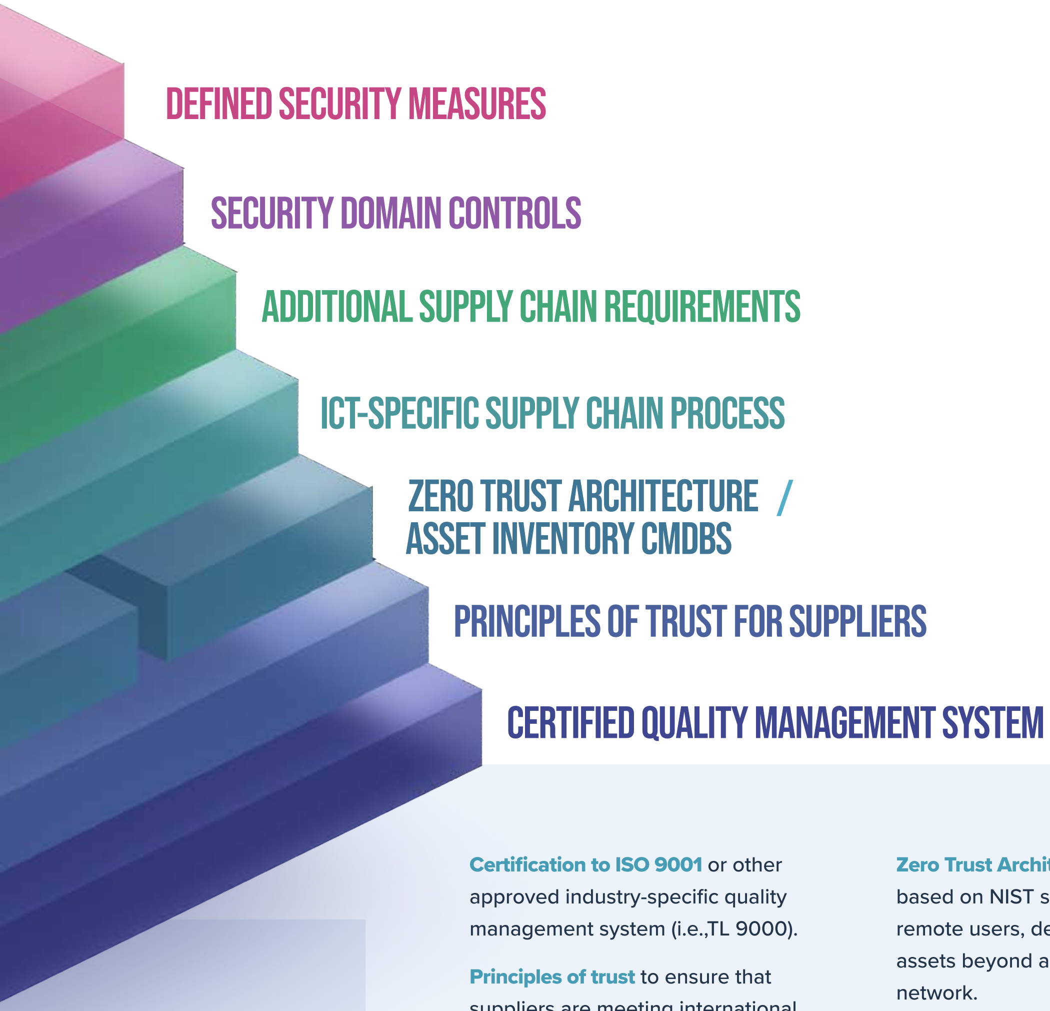
In conducting the landscape analysis, the SCS Workgroup looked at the existing standards and documents from two perspectives:

1. **Necessary quality management components, including:**
    a. A quality management system founded on ISO 9001
    b. Internal audits and corrective action
    c. Management governance, goals, and objectives
2. **Supply chain security requirements and controls, including:**
    a. Asset identification, risk assessment, and mitigation
    b. Security performance benchmarking
    c. Counterfeit parts processes
    d. Software, hardware, and component traceability
    e. Incident response
    f. Secure design, development, and lifecycle management

Based on the detailed landscape analysis and mapping process, the SCS Workgroup found that while each standard has value and merit within its specific area or industry, no one standard was comprehensive or ICT- specific enough to protect the broader ICT supply chain. The SCS Workgroup is therefore integrating the most relevant elements from each standard into the new SCS 9001 Standard. **A snapshot version of the landscape analysis matrix showing each standard and its mapping to coverage areas is available in the annex at the end of this white paper.**

A STANDARDS DEVELOPMENT ARCHITECTURE TO GUIDE THE EFFORT

To help guide the standards development effort and build the teams needed to accomplish the work, the SCS Workgroup created a standards development architecture that defines the internal security requirements that an organization must meet to be standard-compliant and ultimately certified to SCS 9001. The architecture is built from the ground up based on the following key factors:



DEFINED SECURITY MEASURES

SECURITY DOMAIN CONTROLS

ADDITIONAL SUPPLY CHAIN REQUIREMENTS

ICT-SPECIFIC SUPPLY CHAIN PROCESS

ZERO TRUST ARCHITECTURE / ASSET INVENTORY CMDBS

PRINCIPLES OF TRUST FOR SUPPLIERS

CERTIFIED QUALITY MANAGEMENT SYSTEM

Certification to ISO 9001 or other approved industry-specific quality management system (i.e.,TL 9000).

Principles of trust to ensure that suppliers are meeting international government requirements (i.e., violations to anti-corruption or anti-bribery policy, transparency for organizations not having independent Board structures).

Zero Trust Architecture (ZTA) network based on NIST standards that considers remote users, devices, and cloud-based assets beyond an enterprise local network.

Asset inventory configuration management databases (CMDBs) that store information about an environment, all ICT assets, and the relationships among them, even those that are widely distributed.

The SCS Workgroup identified seven **additional ICT supply chain security processes** beyond these key foundational factors that organizations must embody to achieve SCS 9001 compliance.

These include:

- **Incident management** processes to quickly restore service, minimize adverse impact on business operations, and maintain normal levels of service quality and security.
- **Vulnerability management** processes to identify, evaluate, address, and report on security risks within systems and software to prioritize threats and minimize the potential for attack.
- **Risk assessment and mitigation** processes to develop options and actions that enhance opportunities and reduce threats to objectives.
- **Provenance** processes to track diverse origin information for all ICT hardware, software, and components, as well as processes used in the production and delivery of each to determine level of trust.
- **Secure development** processes to implement security analysis into software development lifecycles, integrating security requirements alongside functional requirements and performing risk analysis during the software design phase.
- **Software usage** processes to ensure third-party open-source compliance among all users, integrators, and developers, such as observing all copyright notices and satisfying any license agreements. This is achieved through such practices as scanning for free and open-source software and maintaining code content reports on all software.
- **Counterfeit parts** management processes to identify all assets that are represented as a complete part but that may contain unknown sub-components that have not been pre-screened, enabling the discovery of suppliers potentially producing counterfeit parts that are misrepresented in their origin, security, or quality.

The standards development architecture also includes additional requirements beyond ISO 9001 that are specific to supply chain issues. In addition to the previously defined requirements, a series of security domain controls is also necessary throughout the supply chain. The controls an organization implements to protect its assets will be documented in their Statement of Applicability (SOA).

The SCS Workgroup's standards architecture culminates with a minimum set of measurable performance parameters used to determine compliance and benchmark an organization's ICT supply chain security performance. With a lack of existing ICT-specific quantifiable criteria for measuring supply chain security, and only past events to assess a company's performance, these clearly defined parameters are critical to ensuring a consistent set of criteria that can measure and benchmark the integrity of devices, components, and companies involved across all aspects of the global ICT supply chain. They also provide the foundation for 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. These measurements will be continually and pro-actively updated as technology advances to stay ahead of potential risks rather than responding to issues after they arise.

SCS WORKGROUP TEAMS: AN UNPRECEDENTED EFFORT FOR UNPRECEDENTED TIMES

With relevant elements from industry standards adopted, gaps identified, and a standards development architecture in place, the SCS Workgroup has embarked on the process of developing the new SCS 9001 standard. This was initiated with the activation of an Asset Team that identified and classified all ICT assets to be protected by the new standard. An Initial Requirements Team was also established to determine acceptable risk thresholds and top-level requirements for controls and inventory CMDBs. These initial teams worked with the SCS Workgroup Steering Committee to outline a roadmap for completing the standard and establish the nine additional teams to develop the standard.

These nine SCS Workgroup teams are currently determining and documenting the key requirements for the SCS 9001 QMS standard and certification program:

Oversight – Determines re-use costs for integrating applicable standards, establishes the certification scheme, and identifies auditor qualifications.

Interface to Quality Management System – Determines agreed-upon quality management system requirements, corrective actions, internal audits, and management responsibility beyond ISO 9001.

Control – Determines relevant controls from NIST, CMMC, ISO 27001, CCM and other applicable standards to select, edit, and/or augment in assuring that assets are protected.

Cybersecurity Processes – Determines process requirements for incident management and reporting, risk mitigation, counterfeit parts, legacy network elements, repairs, and maintenance.

Hardware Identification and Traceability – Determines process requirements for identifying and validating hardware component origin, versions, and security.

Software Identification and Traceability – Determines process requirements for identifying and validating free and open-source software code, updates, version, origin, and security.

Secure Development Lifecycle – Determines process requirements for secure coding principles, lifecycle management, software testing, packing and deployment, and other aspects of software development.

Measurements – Defines supply chain security measurements and reporting methods for standard compliance and benchmarking, including information such as number of incidents, effectivity of management processes, secure software testing results, physical security characteristics, and more.

Trust – Identifies principles and determines process requirements for transparency, corporate best practices, and disclosure of relationships with government entities using frameworks determined by international and global non-governmental organizations.

THE CURRENT STATUS

While it was just early 2020 when TIA released its position on ICT supply chain security and the need for industry-driven standards, the recent increase of high-profile attacks called for an accelerated standards development process. This was made possible in part due to adopting the ISO 9001 QMS for the foundation of the SCS 9001 standard, integration of ICT-related aspects from existing recognized standards, and perhaps most importantly, the commitment and dedication of the SCS Workgroup team members.

The result of the work by the SCS Workgroup and its teams is a draft standard that is being used to conduct pilot SCS 9001 certifications with a small set of organizations. Feedback from the pilot program will be incorporated into **Version 1.0 of the standard will be released in Q3 2021.**

THE NEED FOR PRIVATE-PUBLIC COLLABORATION

Recognizing national and international governments' role in the need to secure the ICT supply chain, and the impact of potential policy in this area, TIA's Government Affairs professionals that lead the SCS Workgroup's Trust Team are also concurrently establishing partnerships between governments and the private sector and ensuring bi-partisan support for this critical industry-driven standard.

While government policies and regulations are a necessary and important aspect of ICT supply chain security, especially to prevent risks to national security and public health or safety, global governments recognize that they alone cannot reasonably provide the level of detail required to address all aspects of the ICT supply chain and keep up with the constantly-evolving technology landscape. This is why throughout history, governments have relied on industries like food, drug, and aviation to develop standards that ensure quality and improve security and safety. By supporting the new SCS 9001 QMS standard developed by those entrenched in the development of global ICT products and services, governments will have a more systematic, repeatable framework to address ICT supply chain security and eliminate vulnerabilities to attacks by foreign adversaries.

Government support for the standard also helps eliminate the potential for trade restrictions and regulations around the world that can be wrought with influence from special interest groups and create prohibitive costs for businesses to comply, resulting in decreased competition, innovation, investment, and higher consumer prices. In 2020 alone, at least 38 states, Washington D.C., and Puerto Rico introduced or considered more than 280 bills or resolutions the deal specifically with cybersecurity.xiv Nearly 85% of the world's countries have also enacted or drafted cybercrime legislation that varies widely by region.xv Furthermore, time is of the essence with the threat of hostile attacks on the rise, governments cannot afford to rely on slow bureaucratic policy-making processes, especially during a time of crisis with a pandemic impacting nearly every aspect of life.

The SCS Workgroup's Trust team experts identified a set of trust principles garnered from multiple global government sources related to rule of law, corporate structure, and unfair business practices (i.e., violations to anti-corruption or anti-bribery policies). The team engages with domestic and international government agencies and policymakers, as well as industry forums and regulatory groups, to provide ongoing, transparent status updates and information related to the SCS 9001 standard and trust principles. In addition to these efforts, TIA's Government Affairs also advocates for policies that effectively address supply chain security and hold non-conforming companies accountable without stifling innovation or investment in ICT technology.

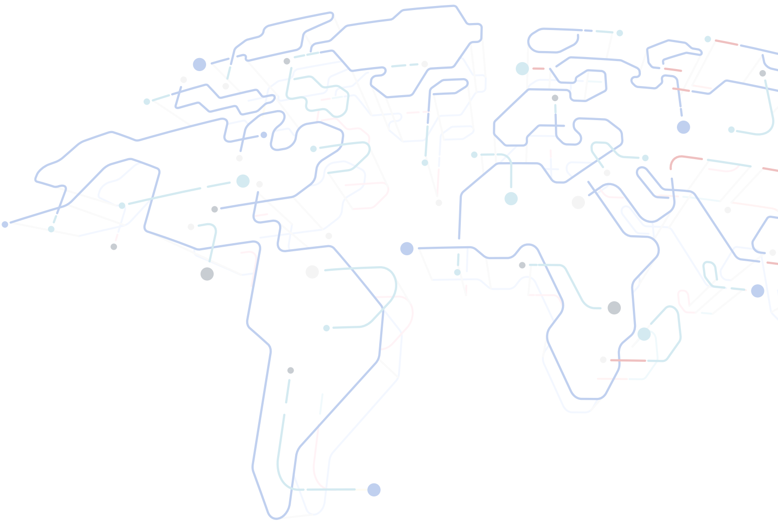
JOIN US IN THE EFFORT

As the first measurable, verifiable supply chain security standard specifically developed for the global ICT industry, the much-needed SCS 9001 standard will provide an industry-driven, processed-based QMS to verify trusted suppliers. Certification to the standard will allow service providers, system integrators, manufacturers, buyers, and suppliers across the global ICT supply chain to verify that the software, hardware, and other ICT equipment they produce and deploy meet critical security benchmarks needed to mitigate risk of cybersecurity breaches and attacks.

Much like the confidence in ISO 9001 and TL 9000 certification, earned over decades, SCS 9001 will ensure confidence in the ICT supply chain among consumers, government entities, and organizations. Knowing that their networks are comprised of hardware, software, and components from SCS 9001-certified and trusted suppliers, business leaders can have peace of mind, ensure operational continuity, and maintain a competitive advantage. SCS 9001-certified companies will also demonstrate to state, local, and federal governments that their networks are comprised of components that have been fully assessed for risk—from hardware and software, all the way to the smallest sub-component.

The work does not end with the initial release of the SCS 9001 QMS standard and certification program. New technologies, broadening the reach of connectivity such as low-latency networking, 5G, advanced Wi-Fi, sensors, and IoT/IIoT implementations are all happening   now. But as the technology continues to advance, threats too will evolve with new cyberattack techniques and back-door mechanisms that can be exploited.

Thankfully, TIA and its members have the experience, the expertise, and the resources to develop the standard and QMS with a comprehensive and transparent third-party certification program. TIA is also the only industry body with a combination of effective government policy advocacy and a deep engineering expertise in developing and maintaining standards, making the organization uniquely qualified to lead the industry in securing the global ICT supply chain.



YOUR EXPERIENCE AND EXPERTISE ARE VITAL

While TIA's leadership and its distinguished Board are prepared and qualified to drive the effort, we cannot do it alone. TIA's extensive and diverse membership represents more than 500 global companies and involves 2,500 active key players and thought leaders representing all aspects of the ICT supply chain. As an ANSI-accredited standard development organization, TIA, with its members, have developed more than 3,600 ICT industry standards that cover a broad range of technologies such as private radio equipment, cellular towers, satellites, data centers, structured cabling, smart buildings, and smart utility networks. TIA encourages any interested party to contact us to join this critical work and help ensure your own expertise is utilized in the development of this important standard.

When it comes to ICT supply chains, simply put, the stakes are higher. The ICT supply chain is too critical, too vast, and too engrained in every other industry not to do everything within reason to minimize the   exposure to cyberattacks and threats and to strengthen national security, secure critical infrastructure, and protect global economic growth. As service providers and suppliers developing and deploying the hardware and software that comprise the world's digital communications infrastructure, we have an obligation to ensure that the devices, equipment, and networks that global businesses and consumers rely on can be trusted and verified.

JOIN US IN HELPING TO SHAPE THE INDUSTRY-DRIVEN SCS 9001 QMS STANDARD AND CERTIFICATION PROGRAM.

→ Contact **supplychainsecurity@tiaonline.org** if you are interested in joining or learning more about SCS 9001.

REFERENCES

i 2021 Report: Cyberwarfare in the C-Suite, Cybersecurity Ventures, January 21, 2021
ii 2020 Open Source Security and Risk Analysis (OSSRA) Report, Synopsys
iii FBI Internet Crime Complain Center (IC3), April 20, 2020.
iv The Cyberwire, Daily Briefing, February 10, 2021.
v 2020 State of the Software Supply Chain Report, Sonatype
vi Biggest Cyber Attacks 2017: How They Happened, Cayptix Security, November 30, 2017
vii The Untold Story of NotPetya, the Most Devastating Cyberattack in History, Wired, August 22, 2018
viii Kingslayer – A Supply Chain Attack, Whitepaper, RSA Research, November 14, 2018
ix Justice Department Charges Five Chinese Members of APT41 over Cyberattacks, September 16, 2020
x Joint Statement by the FBI, CISA, ODNI, and NSA, January 5, 2021
xi Stanford Internet Observatory, Cyber Policy Center, February 12, 2021
xii Securing the Future of a Smart World: Opportunities and Challenges in a 5G Connected Economy, 2019, BPI Network
xiii Breaking Trust: Shades of crisis across an insecure software supply chain, Dr. Trey Herr, William Loomis, Stewart Scott, June Lee, July 26, 2020
xiv NCSL National Conference of State Legislatures, Cybersecurity Legislation 2020
xv United Nations Conference on Trade and Development, April 2020

LANDSCAPE ANALYSIS OF AVAILABLE STANDARDS

			Management System			Proposed Cyber Security Processes and Activities									
Standard	Industry	Standard Owner	QMS with ISO 9001 Foundation	Internal Audits & Corrective Action	Management Governance, Goals, Objectives	Asset Identification, Risk Management & Mitigation	Counterfeit Parts Process	SW, HW, Component PKI & Traceability	Requirements Flow-Down	Incident Response	Cyber Security Metrics	Industry Benchmarking	Security Design Requirements	Secure Development LCM	Control Objectives
AS9100 Series	Aerospace	SAE	✓	✓	✓		✓								
ISO 9000 Series	General	ISO	✓	✓	✓										
ISO 27001	General	ISO		✓	✓	✓			✓	✓		✓	✓	✓	15 Domains, 114 Controls
ISO 27032	General	ISO				✓		Hi Level							Code of Practice 14 Domains, 46 Controls
TL 9000	ICT	QuEST	✓	✓	✓						✓	Supplemental Measurement	✓	✓	
NIST 800-83	General	NIST													18 Domains, LOW - 115, MOD - 159, HIGH - 170
CMMC	General	Carnegie-Mellon		✓	✓ At Level 3	✓			Unknown	✓					17 Domains, 219 Controls L1-15, L2+110, L3+15
FISMA Metrics (2019)	US Federal	NIST										✓ 60 Specified			
TS 16949	Automotive	AIAG	✓					Hi Level							
TSC (AICPA)	Financial Service	AICPA		Implied	Implied	✓			Minimal	✓					65+ Controls
Proposed Solution	ICT	QuEST	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	Controls limited to SCS Effectivity

Other Standards reviewed: ISO 13485, ISO 27002, ISO 27005, ISO 27009, ISO 27017, ISO 27018, ISO 27019, ISO 27035, ISO 27036, ISO 27701, IEEE 15288, TS 23167, IATF 16949, AS 5553, AS 6081, NIST 800-5, NIST 800-53, NIST 800-39, NIST 800-160, NIST 800-161, NIST 800-172, NIST 800-207, O-TPPS, ENISA Guidelines for Securing IOT, BSIMM 11, Secure Agile SDLC. CISA Secure SDLC