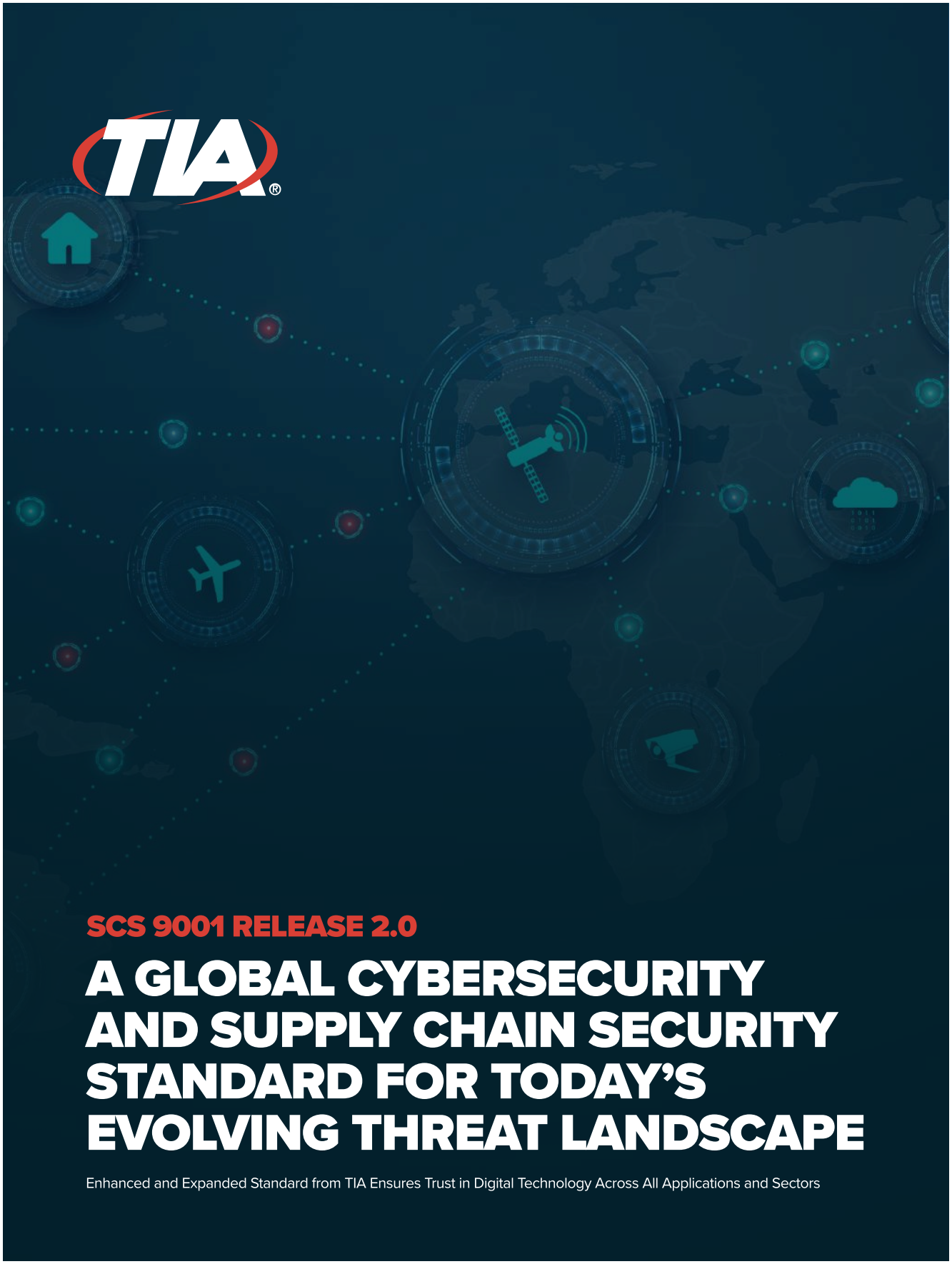


SCS 9001 RELEASE 2.0

A GLOBAL CYBERSECURITY AND SUPPLY CHAIN SECURITY STANDARD FOR TODAY'S EVOLVING THREAT LANDSCAPE

Enhanced and Expanded Standard from TIA Ensures Trust in Digital Technology Across All Applications and Sectors

INTRODUCTION

The Telecommunications Industry Association's (TIA) extensive and diverse membership represents more than 400 global companies. It involves 2,500 key players and thought leaders representing all aspects of the worldwide information and communications technology (ICT) supply chain. As a leading standards organization, TIA has long relied on the expertise of its extensive and diverse membership to develop thousands of technical standards for the ICT industry. Additionally, through its QuEST Forum business performance improvement community, TIA has built the first-ever global Cybersecurity and Supply Chain Security Standard which was released in early 2022. As an industry standards-development organization, TIA continually monitors and improves programs and standards to parallel the latest market trends, technologies, and global economy.

The cybersecurity landscape has evolved significantly since the SCS 9001™ Supply Chain Security Management System was conceived and developed. More frequent and sophisticated attacks are targeting supply chains, consumers, businesses, and government entities due to several global factors, including:

- **Geopolitical unrest —** as a consequence of the Russia-Ukraine conflict, fragile international relations, cybercrime organization expansion and the growth of nationalism and anti-globalization movements
- **Global economic uncertainty —** attributed to surging inflation and debt levels, rising interest rates, and the ever-worsening impact of climate change
- **Expanded attack surfaces —** facilitated by increased digitization and interconnectivity, expanded data access, and the growth of IoT and cloud services
- **Lack of resources —** to implement adequate cybersecurity measures due to skilled labor shortages, gaps in standards and regulations, and budget constraints–especially among small and medium-sized enterprises
- **The exploitation of technologies [by sophisticated non-state and government adversaries] —** such as open-source software, IoT, cloud computing, artificial intelligence (AI), machine learning, and cryptocurrency

Changes in the cybersecurity landscape, combined with feedback via pilot programs, industry leaders, and governing bodies, have called for TIA members to update and expand the scope of its SCS 9001 Cybersecurity and Supply Chain Security standard. The upcoming SCS 9001 Release 2.0 will provide a more comprehensive global cybersecurity and supply chain security standard adaptable to all digital technologies across all applications and industry sectors to serve today's market and extend protection where needed while ensuring alignment with evolving government legislation and industry initiatives.

CYBERCRIME IS EXPANDING WITH TECHNOLOGY AND GLOBAL UNREST

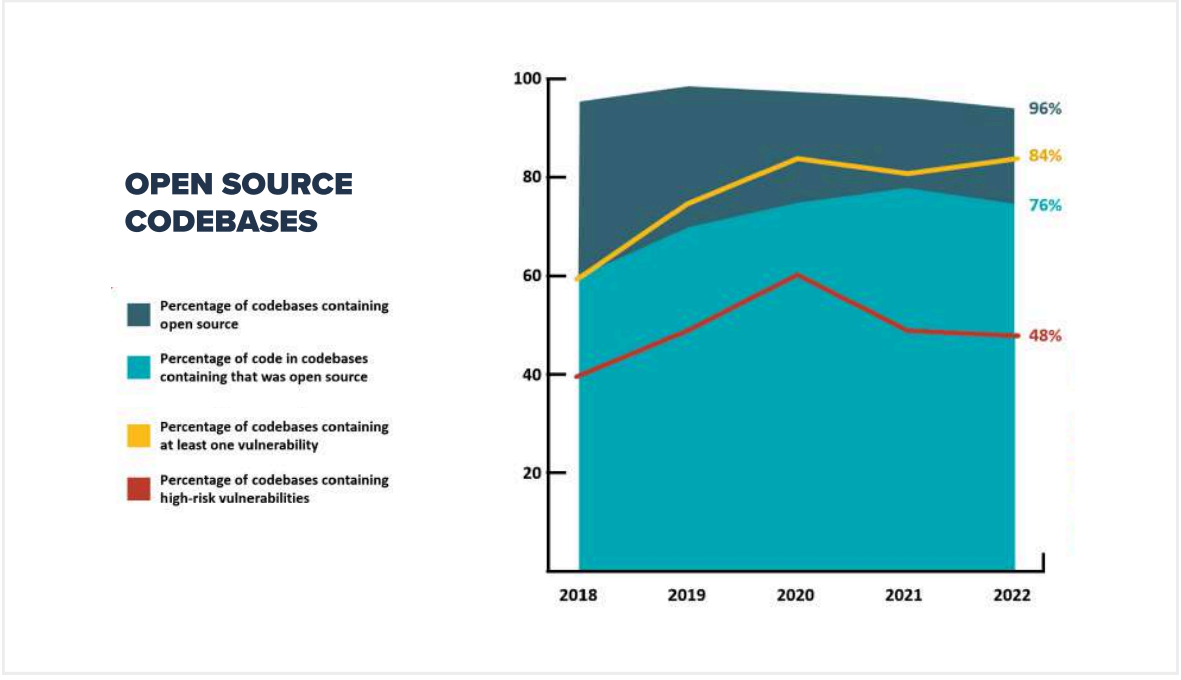
Consumers and businesses today rely on more open and connected IoT devices and always-on applications. As technology continues to expand, so does the cyber threat landscape. At the same time, attack techniques are becoming increasingly sophisticated, with more tools available to aid cybercriminals.

OPEN-SOURCE PROLIFERATION INCREASES VULNERABILITY

Innovation across all sectors increasingly rely on open-source platforms to enable rapid prototyping and deployment, interoperability, and cost savings—from open radio access network (ORAN) 5G mobile communications and autonomous vehicles to financial services, IoT development, and cloud computing.

Open-source software development has become more distributed and ubiquitous in the past decade. More than 95% of all codebases today contain open-source code, and the percentage of open-source code grew 163% in education technology; 97% in aerospace, aviation, automotive, transportation, and logistics; and 74% in manufacturing between 2018 and 2022.[1]

Open-source code stored in public repositories is available for anyone to access and modify, increasing the potential for poorly written or undermanaged code. Open-source code is also often co-created by multiple developers with a range of expertise and without security oversight or standardization. In 2022, more than 80% of analyzed open-source code contained at least one vulnerability, with more than 50% having high-risk vulnerabilities.[1]



[1] 2023 Open Source Security and Risk Analysis Report, Synopsys, Inc.

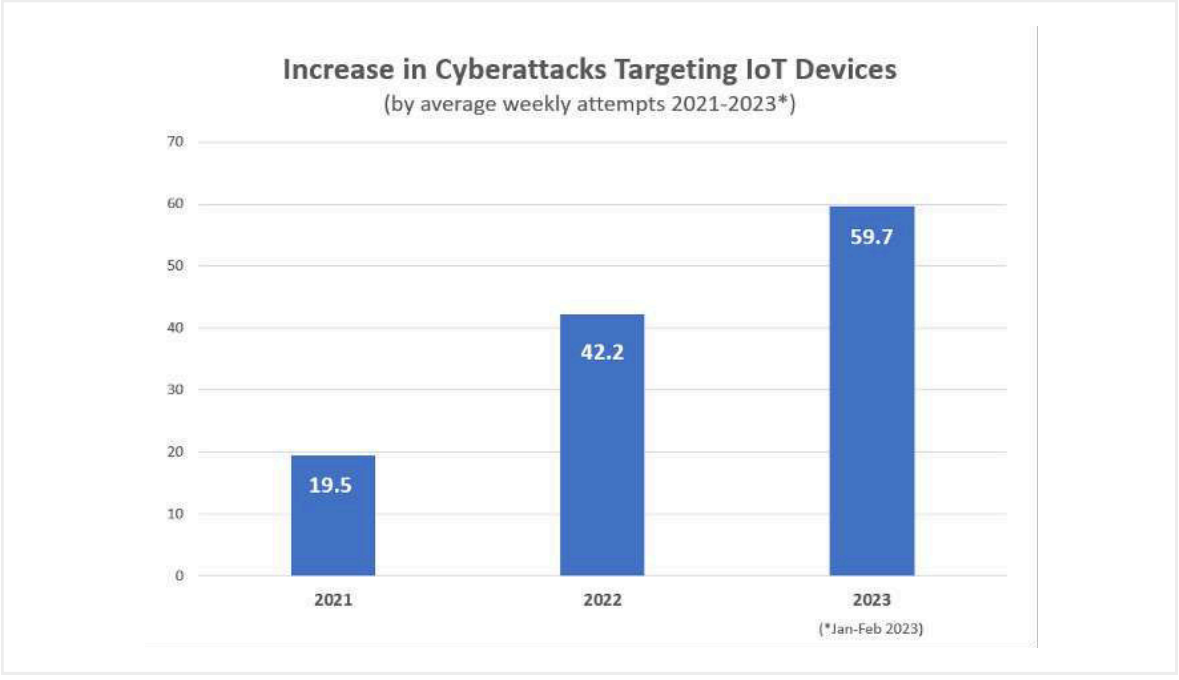
IOT CREATES MORE SUSCEPTIBLE ENTRY POINTS

The ever-increasing range of IoT devices and related services available across commercial, industrial, and consumer sectors is driving widespread adoption, creating more network entry points susceptible to attack. Vendors in the burgeoning and competitive IoT market rely heavily on open-source software to keep prices down and improve speed to market. IoT devices are also typically customized for specific functions with limited computational ability, often inhibiting adequate security measures. Consumer IoT devices (e.g., wearables, smart home, entertainment devices) face additional risks due to a lack of consumer security awareness, insecure home networks, weak passwords, and outdated software.

With these weaknesses, IoT devices are increasingly considered low-hanging fruit to be easily exploited by cybercriminals. High-risk vulnerabilities in IoT-related code bases jumped 130% over the past five years, and the first two months of 2023 saw a 41% increase in attacks targeting IoT devices compared to 2022. [2]

The deployment of broadband access in more regions around the globe will expand connectivity and further drive the IoT market, especially among consumers.

In response to IoT security risks, the US IoT Cybersecurity Improvement Act of 2020 required the National Institute of Standards and Technology (NIST) to set minimum security standards for IoT devices owned and controlled by the federal government. In 2021, US Executive Order (EO) 14028 then directed NIST to initiate pilot programs to educate the public on the security capabilities of IoT devices and identify IoT cybersecurity criteria for a consumer labeling program. NISTIR 8425, Profile of the IoT Core Baseline for Consumer IoT Products, serves as the foundation for the voluntary labeling program. In July 2023, the Biden-Harris administration announced the US Cyber Trust Mark program which will support cybersecurity requirements under NISTIR 8425 and is expected to be up and running in 2024. The Federal Communications Commission, which will administer the



[2] The Tipping Point: Exploring the Surge in IoT Cyberattacks Globally, Check Point Research, 2023

U.S. Cyber Trust Mark program, proposes to implement the NIST Criteria by granting the use of a distinct mark to common consumer devices that meet established cybersecurity criteria, including smart home appliances and devices, entertainment devices, wearables, and more. Several manufacturers and retailers have announced their commitment to the program, including Amazon, Best Buy, Google, LG, Logitech, and Samsung.

Similar international efforts are underway, with more than 156 countries enacting cybercrime legislation and several others drafting new legislation.[3] The UK Code of Practice for Consumer IoT Security and the Product Security and Telecommunications Infrastructure (PSTI) Act requires all manufacturers, importers, and retailers to ensure IoT devices meet required security standards before going to market. A proposed European Union (EU) Cyber Resilience Act (CRA) also protects consumers and businesses purchasing or using products or software with a digital component, including all IoT devices. Singapore launched its own Cybersecurity Labelling Scheme for IoT and has achieved mutual recognition with Finland and Germany.

CLOUD COMPUTING IS A GROWING CYBERCRIME OPPORTUNITY

With digitization and the growth of IoT also comes more cloud-based solutions that increasingly leverage open-source code for application programming interfaces (APIs) to enable integration across diverse workloads. Open-source software vulnerabilities, misconfigurations, storage of large data sets, and lack of access restrictions are giving rise to more cloud-based security threats. Cybercriminals are also becoming increasingly cloud-savvy, targeting public-facing applications and web servers to gain access to off-site cloud platforms, user accounts, and data. According to recent reports, cloud exploitation cases grew by 95%, and nearly 40% of businesses experienced a data breach in their cloud environment in 2022.[4,5]

Cloud providers like Amazon, Microsoft, and Google and cloud alliances are working to define and raise awareness of cybersecurity practices for cloud computing. These cloud providers have also developed architecture frameworks that provide the basis for secure development within their environments. The Federal Risk and Authorization Management Program (FedRAMP) explicitly covers the processing and storage of data in the cloud by federal agencies and their contractors. NIST also has multiple cybersecurity publications for the cloud, including NIST 800-144, Guidelines on Security and Privacy in Public Cloud Computing and NIST 800-210, General Access Control Guidance for Cloud Systems.

EMERGING TECHNOLOGY IS A DOUBLE-EDGED SWORD

Over the past decade, internal organizational network cybersecurity has improved via advanced encryption, authentication, and enhanced awareness. Now, emerging technologies like artificial intelligence (AI) and machine learning (ML) can help identify anomalies to better detect malicious activity and software-related weaknesses. Microsoft's Cyber Signals program leverages AI to analyze 24 trillion security signals, 40 nation-state groups, and 140 hacker groups, successfully blocking over 35.7 billion phishing attacks and 25.6 billion identity theft attempts.[6] Unfortunately, cybercriminals are also now leveraging AI/ML technologies to scan for vulnerabilities, automate malware, crack passwords, analyze stolen data, and formulate content used in social engineering attacks.

The rise in cryptocurrency that uses blockchain technology to enable the secure transfer of digital value in the financial industry is also giving cybercriminals new ways of demanding ransom and facilitating subscription-based ransomware as a service for cybercriminals to launch ransomware attacks.

[3] UN Conference on Trade and Development (UNCTAD), Cybercrime Legislation Worldwide, 2021
[4] 2023 Global Threat Report, CrowdStrike
[5] 2023 Thales Cloud Security Study, Thales
[6] Cyber Signals Report, Microsoft

GLOBAL UNREST IS COMPOUNDING THE PROBLEM

Increasing cybersecurity concerns also mirror rising geopolitical tensions and global economic uncertainty. Cyberattacks are a primary arsenal to maximize infrastructure disruption amidst the Russia-Ukraine conflict and fragile international relations. Cybercriminals also take advantage of nationalism and anti-globalization movements to disrupt the global economy, already plagued by rising inflation, debt levels, and interest rates. In March of 2023, the White House released a National Cybersecurity Strategy to collaborate with foreign allies and partners to advance shared goals and provide support to galvanize global cyber defense efforts. US government agencies directly support Ukraine to identify and protect against cyberattacks and bolster response and recovery. Key international efforts also include the US-EU Ransomware Working Group, the US-Republic of Korea Ransomware Working Group, and several other joint cybercrime task forces and working groups.

SECURING THE GLOBAL SUPPLY CHAIN IS MORE VITAL THAN EVER

Addressing vulnerabilities at the foundation of software and hardware development is more vital than ever. The software and hardware components and subcomponents of equipment, devices, and networks come from multiple suppliers and resources that comprise a complex, global supply chain. Attacks on software supply chains are increasing dramatically, with one State of the Software Supply Chain report showing an average 700% jump in open source supply chain attacks between 2018 and 2022.[7] With these attacks targeting ubiquitous components and development processes across multiple solutions and market sectors, supply chain attacks quickly escalate across thousands of networks and impact millions of users.

[7] Sonatype's 8th annual State of the Software Supply Chain Report, October 2022

In response to the need for supply chain security, the 2021 US Executive Order (EO) 14028 directed NIST to issue guidance identifying practices that enhance the software supply chain security. In September 2022, the Office of Management and Budget (OMB) issued Memorandum M-22-18 requiring federal agencies to comply with the NIST guidance. In addition, the US Cybersecurity and Infrastructure Security Agency (CISA), in partnership with national security and counterintelligence agencies, released the Enduring Security Framework that provides guidelines for software vendors on implementing secure development processes. As a result of these efforts, many federal government stakeholders and partners must attest that they have an acceptable cybersecurity and supply chain risk management (C/SCRM) plan in place, including all Eligible Entities and sub-grantees of the Broadband Equity, Access, and Deployment (BEAD) Program. 2022 also saw the introduction of the Securing Open-Source Software Act, a proposed bipartisan legislation that increases CISA's focus on open-source code risks. It requires software suppliers to the federal government to attest to the security of their code and produce software bills of material (SBOMs) to track supply chain threats.

SCS 9001 IS A TECHNOLOGY-AGNOSTIC GLOBAL STANDARD

The government's increased focus on cybersecurity and supply chain security will help boost defenses in the public sector. However, deciphering and complying with new legislation, often in addition to industry-specific standards and guidelines, can be overwhelming. Plus, the fact remains that the private sector accounts for a substantial portion of the world's equipment, devices, and networks and spans multiple industries and regions. The global consumer market alone accounted for roughly 60% of all connected IoT devices in 2020 and is projected to remain at that level through 2030.[8]

Many of the cybersecurity initiatives underway also focus on common vulnerabilities such as consumer awareness, device identification, secure access, protection of personal data, and automatic software updates and do not get to the foundation of software and hardware development deep within the global supply chain.

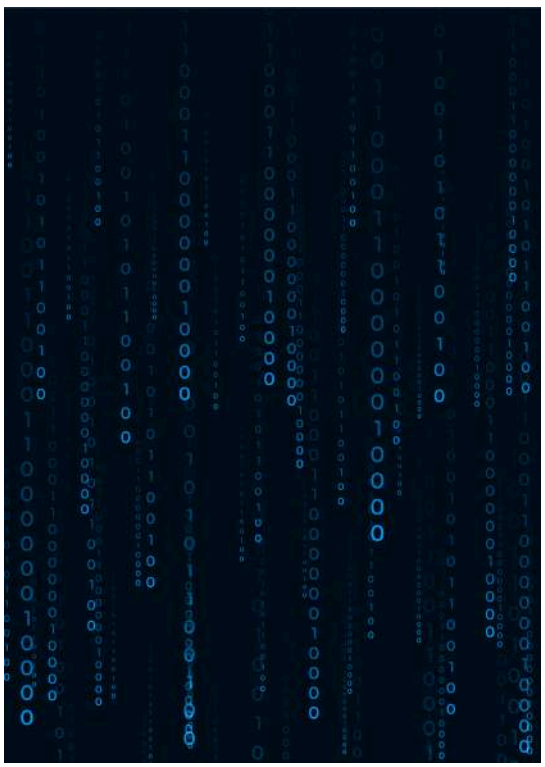
Since 2022, TIA's SCS 9001 Cybersecurity and Supply Chain Security Standard has provided a global umbrella for baseline cybersecurity requirements that apply to all aspects of the vast, complex supply chain across all public and private sectors. While no single standard is sufficient for securing all components and applications, SCS 9001 provides a straightforward means for network operators, service providers, system integrators, manufacturers, buyers, suppliers, and consumers across the global supply chain to ensure that the software, hardware, and other technology components they produce, purchase, and deploy meet critical security benchmarks to mitigate the risk of cybersecurity attacks.

SCS 9001's underlying process-based architecture is a systematic, repeatable framework that integrates security requirements alongside functional requirements in the design, development, and delivery of equipment and devices. This includes comprehensive provenance, risk assessment, and software usage processes for pre-screening, tracking, analyzing all components and subcomponents, including free and open-source software code content, and ensuring compliance among all suppliers. SCS 9001 also includes processes for identifying, addressing, and reporting security risks to minimize the potential for attack and adverse impact on consumers and businesses.

[8] Statista, Number of IoT Connected Devices Worldwide 2019-2021, with Forecasts to 2030

SCS 9001 RELEASE 2.0 RESPONDS TO THE NEED

Since the release of SCS 9001, TIA has diligently monitored the cybersecurity landscape and evolving threats and vulnerabilities while maintaining ongoing relations with government agencies and industry leaders to stay abreast of and involved in federal policy, legislation, and industry initiatives. Through initial SCS 9001 pilot programs and engagements, TIA has also worked with network operators, service providers, system integrators, manufacturers, security consultants, buyers, and suppliers across the global supply chain to gather feedback and understand their evolving cybersecurity challenges, concerns, and needs.



As a result of this ongoing effort, TIA is updating and expanding the SCS 9001 standard. The upcoming SCS 9001 Release 2.0 will provide a more comprehensive, adaptable standard that ensures alignment with government policies and industry initiatives while providing a simple, unified architecture with baseline cybersecurity and supply chain security requirements that apply to all stakeholders across all sectors. SCS 9001 Release 2.0 is enhanced to provide:

- **Expanded coverage —** for the provenance and development of any technology, including emerging IoT and cloud-based applications
- **Expanded coverage —** for global supply chain procurement, shipping, and logistic policies and procedures
- **Improved support —** for government policy and legislative requirements
- **Updated mapping controls —** to other global standards and publications

In addition, TIA reorganized and reformatted SCS 9001 Release 2.0 to improve overall useability. The SCS 9001 Release 2.0 decouples from ISO 9001 quality requirements in recognition that business entities responsible for quality differ from those responsible for cybersecurity.

SCS 9001 Release 2.0 provides data center and cloud providers, network operators and service providers, equipment and device manufacturers and suppliers, and designers and integrators confidence that current and future applications, equipment, and devices have been thoroughly assessed to prevent cyberattacks. It provides peace of mind for these stakeholders to deploy technology without compromising the safety and livelihood of consumers and business customers. At the same time, commercial, industrial, and government entities can ensure that solutions from their SCS 90001-certified vendors are inherently protected against cyberattacks that can disrupt business continuity, damage reputations, or endanger national security.

TO LEARN HOW SCS 9001 RELEASE 2.0 CAN ENSURE CYBERSECURITY AND SUPPLY CHAIN SECURITY FOR YOUR BUSINESS:

CONTACT

SUPPLYCHAINSECURITY@TIAONLINE.ORG