Version: 0.1
Last Update: July 9, 2023

A COMPARISON OF TIA QUEST FORUM'S SCS 9001 CYBER AND SUPPLY CHAIN SECURITY MANAGEMENT SYSTEM WITH THE CONSUMER TECHNOLOGY ASSOCIATION'S ANSI/CTA-2088

EXECUTIVE SUMMARY

In July 2023, the FCC announced the creation of the US Cyber Trust Mark, a cybersecurity labeling program for Internet of Things (IoT) devices aimed at improving the security and resilience of network-attached consumer devices with a set of baseline requirements. While this program is expected to be implemented in late 2024, companies can take steps now to evaluate their security posture by using existing cybersecurity standards.

This Technical Bulletin compares 2 prominent standards:

1. Consumer Technology Association (CTA) Standard ANSI/CTA -2088 and titled "CTA Standard Baseline Cybersecurity Standard for Devices and Device System"
2. Telecommunications Industry Association's (TIA) SCS 9001 Cyber and Supply Chain Security Management System

INTRODUCTION TO THE TELECOMMUNICATIONS INDUSTRY ASSOCIATION (TIA)

The Telecommunications Industry Association (TIA), the trusted industry association for the connected world, represents more than 400 global companies that enable high-speed communications networks and accelerate next-generation ICT innovation. Through leadership in U.S. and international advocacy, technology programs, standards development, and business performance improvement solutions, TIA and its members are accelerating global connectivity across every industry and market. TIA is accredited by the American National Standards Institute (ANSI) and is active in developing and promoting international standards. TIA QuEST Forum brings together companies from around the world who manufacture, deploy and operate cutting edge networks, to develop process-based industry standards and tools to improve business performance and to address the challenges that come with digital transformation, new business models, innovation, and increasing competition.

TIA's QuEST Forum community built and maintains the ICT industry's most prominent quality standard – TL 9000. As part of our commitment to ensuring global networks are reliable, trusted and secure, TIA QuEST Forum has released the "SCS 9001 Cyber and Supply Chain Security Management System", a process-based standard focused on supply chain security for the global Information and Communication Technology (ICT) industry.

SCS9001 is the first comprehensive, measurable, and independently certifiable process-based supply chain security standard for the ICT industry and benchmarks performance to drive continuous improvement. This standard provides value to network operators of all types and developers and manufacturers of products and services used within those networks.

INTRODUCTION TO ANSI/CTA-2088

The Consumer Technology Association (CTA)® is a trade association representing the U.S. consumer technology industry. The CTA has developed the ANSI/CTA-2088 standard with a focus of improving the cybersecurity of Consumer IoT devices. The CTA is now targeting additional areas building on the current standard with examples such as ANSI/CTA-2088.1 which is named Baseline Cybersecurity for Small Unmanned Aerial Systems.

ANSI/CTA-2088 was released in December 2020 and was developed by the CTA R14 Cybersecurity and Privacy Management Committee.

The purpose of the standard is described in the Scope:

This standard specifies baseline Device Security capabilities and related organizational Security capabilities and recommendations for Devices and Device systems, including for individual connected Devices, Endpoint Devices, components, hardware modules, chips, software, sensors or other operating components.

ANSI/CTA-2088 is a 38-page document with a total of 110 requirements. Of the total requirements, 102 are focused on device security and 8 requirements target manufacturer responsibilities such as device end of service life, how updates are made available, and vulnerability management.

The following table provides an overview of the requirements:

CATEGORY	PRIMARY DESCRIPTION	SECTION	REQUIREMENTS
Device Identifiers	Ability to self-report device identi-ty.	5.1	2
Secured Access	Protection of device operational and management capabilities	5.2	2
Credentials and Logins	Using credentials to secure access to and from any device	5.2.1	14
Validate Certificates	Proper validation of certificates	5.2.2	16
User Interfaces, Console Ports and Remote Management Protocols	Securing interfaces used for remote management of the device	5.2.3	6
Web Services	Securing access to web sites and cloud services	5.2.4	3
Data In Transit is Protected	General introduction to ensure protection of all data in transit	5.3	_
Physical Networking Technolo-gies Supporting Ethernet MAC	Ensuring protections over physical networks using Ethernet MAC layer technologies.	5.3.1	3
Physical Networking Technolo-gies Without Ethernet MAC	Ensuring protections over non-ethernet MAC layer technologies such as Zigbee or Z-wave	5.3.2	1
Link-Layer Application Proto-cols	No restrictions are placed over link-layer protocols used on the local LAN	5.3.3	0
Encrypting IP Transport Pro-tocols	Encrypting communications used over TCP/IP and/or UDP/IP proto-cols	5.3.4	5

CATEGORY	PRIMARY DESCRIPTION	SECTION	REQUIREMENTS
Integrity	Authenticating data in transit	5.3.5	1
Data at Rest is Protected	Protection of stored data and cre-dentials	5.4	11
Industry Accepted Protocols are Used for Communications	Use of common, current and secure protocols	5.5	3
Data Validation	Checks for input data to ensure va-lidity	5.6	7
Event Logging	Logging important events detected by the device	5.7	4
Cryptography	Use published and proven crypto-graphic meth-ods	5.8	12
Patchability	Ability to update a device's configu-ration and software	5.9	4
Reprovisioning	The ability to securely reconfigure a device includ-ing returning a device to factory defaults	5.10	8
Vulnerability Submission and Han-dling	Manufacturer requirements for par-ticipating in industry threat-sharing programs and handling of unsolicit-ed notifications of potential vulner-abil-ities	6.1	4
EoL/EoS Updates and Disclo-sure	Providing guidance on how to re-ceive product updates and disposi-tion of products no longer support-ed.	6.2	2
Device Intent Documentation	Manufacturer provided information on product network usage and stor-age of sensitive data.	6.3	2

INTRODUCTION TO TIA SCS 9001

SCS 9001 is a cyber and supply chain security management standard developed by members of the ICT industry for the ICT industry. SCS 9001 was developed to provide assurance of the proper operational hygiene of network operators and vendors in delivering products and services that are inherently more secure.

SCS 9001 is approximately 150 pages in length. It contains 116 high-level requirements with most being multi-part. When fully considered, there are nearly 800 individual requirements. Further, SCS 9001 contains 60 controls and specifies 7 measurements for those organizations electing to participate in TIA's Industry Benchmarking program.

SCS 9001 was developed to help evaluate and provide higher assurance that vendors:

- operate their businesses with integrity, transparency and are trustworthy,
- conduct all aspects of operations with a high level of security consideration,
- develop products and services with security built in from conception and considered through-out the entire lifecycle,
- have made requisite investments to support products through their entire lifecycle, including the ability to identify, mitigate and resolve vulnerabilities found post-deployment.

SCS 9001 DIFFERENTIATION TO ANSI/CTA-2088

ANSI/CTA-2088 focuses on security improvements in the design and operation of network-attached consumer devices. SCS 9001 is a broad and in-depth standard that provides the same coverage for many of the security requirements described within ANSI/CTA-2088, but with a much more comprehensive set of requirements in assuring operating principles of vendors and the security of their supply chains.

The types of coverage offered by SCS 9001 includes the following examples, in no particular order[1]:

- Corporate Principles of Trust
- Zero Trust Network Architecture
- Asset Inventory DB and Management
- Understanding the needs and expectations of interested parties
- Relevant Legal, Statutory, Regulatory, or Contractual Requirements
- Leadership and commitment
- Top management governance
- Customer security requirements
- Establishing the security policies
- Media Management Policy
- Human Resource (HR) Security Policy
- Acceptable Use of Assets Policy
- Workspace Policy
- Access Control Policy
- Least Privilege Policy
- Asset Management Policy
- Mobile Device Policy
- Bring Your Own Device (BYOD) Control Policies
- Cryptographic Control Policies
- Counterfeit Parts Mitigation Policy
- Management Responsibility for Supply Chain Security
- Security Program Planning
- Asset Inventory
- Ownership of Assets
- Residual Risk Information Availability
- Asset Classification
- Supply Chain Security Risk Identification
- Security Risk Analysis
- Supply Chain Security Risk Treatment
- Business Impact Analysis
- Business Continuity Planning
- Management of security objectives
- People, Infrastructure, and Environment
- Monitoring, verification, and validation of resources
- Determining and Ensuring Competence
- Security Awareness Training
- Internal and external Communications
- Customer Communication Methods
- Organization Feedback
- Control of documented information
- Protection of Personally Identifiable Information (PII)
- Audit Logging
- Product Life Cycle Model
- Technical Vulnerability Management
- Secure Network Planning
- Secure Systems Planning
- Secure Wireless Network Procedures
- Maintenance of Organizational Systems
- Information Backup

- Problem Escalation
- Problem Report Feedback
- Product Replacement
- Notification of Critical Security Problems
- Notification of Critical Service Disruption
- Identification of Customer and Stakeholder Security Needs
- Design and development of products and services
- Secure Development Models
- Security Requirements of Project Planning
- Security Test Planning
- Integration Planning
- Requirements Traceability
- Security Test Verification and Validation Process Controls
- Software Provenance
- Software Bill of Materials (sBOM)
- Hardware Provenance
- Hardware Bill or Materials (BOM)
- Design and Development Change Management Process
- Informing Customers of Security Design Changes
- Security Vulnerability Resolution Configuration Management
- Component Substitutions
- Supplier Selection
- Data Sub-processors
- Supply Chain Provenance
- Extent of Control of Critical Supplier(s)
- Verification of Externally Supplied Products
- Verification of Externally Supplied Services
- Supply Chain Security Operational Processes
- Network Security Requirements Definition Process
- Network Architecture Definition Process
- Secure Network Operations
- Secure Systems Operations
- Event and Incident Management Process
- Incident Reporting
- Monitoring Access Control
- Software Malware Protection
- Secure Logistics Processes
- Disposal Process
- Release of products and services
- Control of nonconforming outputs
- Nonconformance records
- Performance evaluation
- Monitoring, measurement, analysis and evaluation
- Security Management System Evaluation
- Security Process Measurements
- Required Security Measurements
- Internal Audit Program
- Corporate Governance

CONCLUDING REMARKS

ANSI/CTA-2088 is an important standard that prioritizes enhancing the cybersecurity and resilience of network-attached consumer devices. It places a strong emphasis on secure communications, as well as data and access controls.

SCS 9001 has been purpose-built to address today's cyber and supply chain security challenges, providing coverage for many different types of networks and the devices operating within those networks. It is a powerful standard developed by premier organizations operating within the ICT industry with flexibility to be applied to the needs of a variety of industries.

The challenge of cyber and supply chain security is significant with no single standard or work being sufficient to address all needs. ANSI/CTA-2088 and SCS 9001 can be used together as an effective combination to provide a higher level of security and resilience for the consumer device (IoT) industry.

REFERENCES

[1] This is a partial list. SCS 9001 is a very comprehensive standard. Identifying and describing every requirement in detail is beyond the scope of this Tech Bulletin.

- Consumer Technology Association Web Site: https://www.cta.tech/
- Telecommunications Industry Association Web Site: https://tiaonline.org/
- CTA's ANSI/CTA-2088 standard: https://iotsecuritymapping.com/wp-content/uploads/2022/05/ANSI-CTA-2088-Final.pdf
- Information related to TIA's SCS 9001 Standard: https://tiaonline.org/what-we-do/technology-programs/supply-chain-security/