TIA QuEST Forum
Telecommunications Industry Association
TECHNICAL BULLETIN
TIAonline.org / @TIAonline

How SCS 9001 Supply Chain Security Standard Operationalizes EO 14028.

April 21, 2022

Executive Summary

The United States Government and its various agencies are aggressively focused on improving the resiliency of the nation's critical infrastructure (CI), IT assets and networks in response to increasing cyberattacks. A new strategic focus and approach to cybersecurity, with a desired end state of layered cyber deterrence, is required to reduce the probability and impact of cyberattacks of significant consequence. Additionally, a number of Executive Orders and positioning papers have been released over the past few years to address the need for government and private industry to cooperate and significantly improve the cyber security of all networks.

This TIA Bulletin gives an overview of EO 14028 and how the TIA QuEST Forum SCS 9001 Supply Chain Security standard operationalizes the goals of the Executive Order.

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 solutions, TIA and its members are accelerating global connectivity across every industry and market. TIA is accredited by the American National Standards Institute (ANSI).

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 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 Executive Order 14028

Executive Order 14028 was issued on May 17, 2021. It is organized into 10 sections, an overview of each follows:

- **Section 1. Policy:** this section introduces the problems being faced and sets the tone for the remainder of the Order. It identifies the risks of cyber-attacks, the need for the government to improve the security of its networks and IT operations with bold changes and expresses the need for government and private industry to cooperate on meeting the goals of improved cyber-security.

  The importance of this EO is summarized by the statement:

  "*It is the policy of my Administration that the prevention, detection, assessment, and remediation of cyber incidents is a top priority and essential to national and economic security.*"

- **Section 2. Removing Barriers to Sharing Threat Information:** this section states the need to improve the sharing of threat information. Covered topics include standardizing on contractual requirements with service providers, expectations that network operators provide threat information and report on cyber incidents, and requirements that service providers cooperate with government agencies investigating cyber- attacks. Further, this section requires that CISA collect and maintain a database of all incidents.
- **Section 3. Modernizing Federal Government Cybersecurity:** this section mandates that the government modernize its approach to cybersecurity. Topics covered include adoption of security best practices, moving towards a Zero Trust Architecture, securing cloud services, consolidation of cybersecurity information to

improve analytics and risk assessment, and making requisite investments in achieving these goals.

This section also identifies FedRAMP as a target for modernization and that they should identify relevant compliance frameworks and map requirements of their vendor authorization process to those frameworks.

- **Section 4. Enhancing Software Supply Chain Security:** this section starts with a critical view of the current state of commercial software:

  "The development of commercial software often lacks transparency, sufficient focus on the ability of the software to resist attack, and adequate controls to prevent tampering by malicious actors".

  This section identifies 'critical software' as a specific concern. Critical software is defined as performing functions such as allowing elevated system privileges or direct access to networking and computing resources.

  Additionally, this section has a relatively heavy focus on the software supply chain and integrity of the software development environment. The EO sets expectations in areas such as delivery of Software Bills of Materials (sBOMs), evidence of provenance of software, establishment of secure development environments and controlled access to those environments and the use of automated vulnerability assessment tools.

  Finally, this section addresses issues around consumer software and IoT up to and including the potential for a consumer labeling program to be considered.

- **Section 5. Establishing a Cyber Safety Review Board:** this section states that a Cyber Safety Review Board be established by the Secretary of Homeland Security in consultation with the Attorney General. The board is intended to review significant cyber incidents. The Board's membership includes representatives of the Department of Defense, the Department of Justice, CISA, the NSA, and the FBI, as well as representatives from appropriate private-sector cybersecurity or software suppliers as determined by the Secretary of Homeland Security.

- **Section 6. Standardizing the Federal Government's Playbook for Responding to Cybersecurity Vulnerabilities and Incidents:** this section promotes the standardization of cybersecurity vulnerability and incident response procedures which today differ across various government agencies. A playbook is to be delivered defining a standard set of operational procedures to be used in planning and conducting cybersecurity vulnerability and incidence response.
- **Section 7. Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Networks:** this section promotes early detection of cybersecurity incidents on government networks. It promotes proactivity in searching for vulnerabilities prior to an incident occurring.
- **Section 8. Improving the Federal Government's Investigative and Remediation Capabilities:** this section focuses on the collection of information from both on-premise systems and networks as well as those of Communications Service Providers (CSPs) providing services to the government. Expectations are made that all service providers collect and maintain incident data and provide such data at the request of Secretary of Homeland Security through the Director of CISA and to the FBI, consistent with applicable law.
- **Section 9. National Security Systems:** this section sets requirements for National Security Systems such as those operated by the Department of Defense that are equivalent to or exceed the requirements of this EO.
- **Section 10. Definitions:** this section provides definitions used through-out the EO.
- **Section 11. General Provisions**: this section provides clarifying comments and disclaimers.

How SCS 9001 Helps to Achieve the Goals of Executive Order 14028

The following table provides an overview of specific requirements of SCS 9001 that align with the requirements of Executive Order 14028.

The provided examples are intended to be illustrative of the alignment between SCS 9001 and this Executive Order and not all inclusive.

U.S. Executive Order 14028	TIA QuEST Forum SCS 9001
Section 1. Policy	SCS 9001 was developed in response to challenges the ICT industry faces in improving security, and specifically within the supply chains of ICT vendors. Virtually all of the specific requirements in this EO directed at network operators and software developers are addressed within SCS 9001. Certification to SCS 9001 will improve the inherent security of products deployed in federal, public and private networks, while increasing the integrity of suppliers.
Section 2. Removing Barriers to Sharing Threat Information	SCS 9001 support for requirements of this section: • Vendors must establish Technical Vulnerability Management processes to identify, evaluate, treat and report on security vulnerabilities • Vendors must establish Incident Management processes to restore normal operations as quickly as possible while minimizing the adverse impacts of cyberattacks.
Section 3. Modernizing Federal Government Cybersecurity	SCS 9001 support for requirements of this section: • Requiring a plan for achievement of a ZTA. • Multi-factor authentication for access to systems. • Ensuring data is encrypted, both in transit and at rest.

U.S. Executive Order 14028	TIA QuEST Forum SCS 9001
Section 4. Enhancing Software Supply Chain Security	SCS 9001 support for requirements of this section: • Establishment of secure development environments with controlled access to those environments, separate from production environments. • Providing Software Bill of Materials (sBOMs) • Evidence of provenance of software including 3rd party components with traceability • The use of automated vulnerability assessment tools. • Vulnerability assessment of all open-source software integrated into the product
Section 5. Establishing a Cyber Safety Review Board	SCS 9001 requires that network operators and vendors deploy best practices for securing their business operations and ensuring the integrity of their products and services. Those certified to SCS 9001 are likely well suited to participate in the Cyber Safety Review Board referenced in this section.
Section 6. Standardizing the Federal Government's Playbook for Responding to Cybersecurity Vulnerabilities and Incidents	This section sets requirements for the development of Cybersecurity Incident & Vulnerability Response Playbooks to be used by Federal Contractors. Certification to SCS 9001 will help organizations deploy best practices that aligns well with the expectations defined within these playbooks. Examples include: • Establishing security awareness training. • Establishing Business Impact Analysis • Creating a Business Continuity Plan • Monitoring infrastructure for anomalous traffic patterns and system access • Deploying and operating a secure network infrastructure. • Maintaining documented information for detected critical problems and notifying customers of such problems • Effective and consistent system patching

U.S. Executive Order 14028	TIA QuEST Forum SCS 9001
Section 7. Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Networks	This section is primarily directed at government agencies. Vendors who certify to SCS 9001 will be viewed as credible suppliers aligned with government policies.
Section 8. Improving the Federal Government's Investigative and Remediation Capabilities	This section is primarily directed at government agencies. Vendors who certify to SCS 9001 should be viewed as credible suppliers aligned with government policies. In particular, this section details policies for logging, log retention and log management. SCS 9001 has extensive logging requirements exactly in support of such needs.
Section 9. National Security Systems	This section concentrates on highly secure systems and provides for potential exceptions to EO 14028 as necessitated by the special needs of those networks and systems. Certification to SCS 9001 will likely be an effective baseline for the unique requirements of these networks and systems.
Section 10. Definitions	This section provides definitions used within the order. Specifically, SBOM and Zero Trust Architecture are defined. SCS 9001 aligns with these definitions.
Section 11. General Provisions	There is nothing in this section applicable to SCS 9001, nor should there be.

References

- Executive Order 14028: eo-14028.pdf (fas.org)
- TIA QuEST Forum SCS 9001 Information: Supply Chain Security Standard: SCS 9001 (tiaonline.org)
- NIST definition of critical software: Critical Software Definition | NIST

Questions? Want to get involved or learn more about SCS 9001?
Visit: https://bit.ly/SCS9001
Send us an email: supplychainsecurity@tiaonline.org

This document is not a Standard or TSB and does not modify any existing standards. This document is solely meant to communicate ideas and general information to industry.