TIA | QuEST Forum

# How SCS 9001 Supply Chain Security Standard Aligns with the Prague Proposals

## Summary

Trade and standards organizations along with government agencies from around the world are developing proposals in response to the increasing threat of cybersecurity. One such body is the National Cyber and Information Security Agency, the organizer of the Prague 5G Security Conference and publisher of recommendations commonly known as the Prague Proposals.

This paper demonstrates how the Telecommunications Industry Association (TIA) standard *SCS 9001™ Supply Chain Security Management System* operationalizes the Prague Proposals from *The Chairman Statement on Cyber Security of Emerging and Disruptive Technologies* (December 1, 2021) and *The Chairman Statement on Telecommunications Supplier Diversity* (November 30, 2021).

## Introduction to Prague 5G Security Conference[1]

The Prague Proposals were endorsed during the first Prague 5G Security Conference in May 2019. The Prague Proposals is a set of recommendations on both technical and non-technical risks that States should consider when planning, building, launching, and operating their 5G infrastructure.

The Prague 5G Security Conference is a leading global forum dedicated to the security of 5G infrastructure that gathers government officials, representatives of international and regional organizations, researchers from universities and think-tanks, and subject-matter experts. The conference is organized by the National Cyber and Information Security Agency of the Czech Republic.

The Prague 5G Security Conference was founded in 2019 with the aim to raise awareness about the importance of 5G infrastructure in the context of national and international security. The overall overarching aim of the conference in the long-term is to foster international dialogue on the strategic significance of 5G infrastructure and encouraging participants to share best practices, approaches and lessons learned.

At the end of the conference, the Prague Proposals on Cyber Security of Emerging and Disruptive Technologies (EDTs) were presented. The participating countries agreed on possible principles for a future approach to disruptive technologies. The document mentions, for example, an approach based on consideration of technical and non-technical risks, supply chain security, transparency, trustworthiness, and diversification, as well as democratic and ethical values in the context of 5G infrastructure.

This year's conference also resulted in the second set of proposals, the Prague Proposals on Telecommunications Supplier Diversity.

[1] Excerpts from this introductory section are taken from the Prague 5G Security Conference web site at prague5gsecurityconference.com – Prague 5G security conference

## Introduction to the Telecommunications Industry Association (TIA)

TIA ensures optimum performance, security and sustainability of products and services used throughout the global Information and Communication Technology (ICT) industry. Through its Standards Development, Technology Programs, QuEST Forum and Government Advocacy communities, TIA provides a neutral ground for the industry to collaborate and solve common challenges.

TIA's 400+ member and participant companies have powered advancements in communications for 90+ years.

The TIA QuEST Forum has announced the "*SCS 9001™ Supply Chain Security Management System*", a process-based standard focused on supply chain security for the global ICT industry. The need for ICT and network supply chain security has increased as connectivity expands globally and SCS 9001 is a powerful and complementary addition to the quality management processes in place at 5G and other service providers and their suppliers.

While TIA's heritage is in addressing the needs of telecom network operators and their suppliers, the communications landscape has changed and accordingly, so must the standards by which future products used in communications applications must conform. SCS 9001 is an example of such a standard and it operationalizes many of the recommendations outlined in the Prague Proposal.

The following tables explain how SCS 9001 operationalizes the specific cyber security protocols set forth at the Prague 5G Security Conference.

| Prague Proposal: Cyber Security of Emerging and Disruptive Technologies | TIA QuEST Forum SCS 9001™ |
|---|---|
| **RISK-BASED APPROACH** | |
| The Prague Proposals assert that risk assessments be made on a continuous basis with adoption of adequate risk mitigation measures. | SCS 9001 encourages supply chain security across the complete product lifecycle through the promotion of risk-based thinking, and that organizations perform and produce on request an analysis of security risks that cover but are not limited to supply chain, asset management, human resources, physical and environmental, communications and operations, access control, and information systems acquisition, product development, and maintenance. |
| **PRINCIPLES-BASED APPROACH** | |
| The Prague Proposals encourages that security outcomes under various scenarios be defined but that flexibility be promoted in achieving such outcomes while not hindering innovation and investment. | SCS 9001 is a flexible standard, enabling organizations to certify elements to their specific needs while supporting numerous underlying Quality Management Systems upon which SCS 9001 builds. Adoption of SCS 9001 will provide organizations a competitive advantage in being able to deliver products and services with higher certainty as to the security of those products and services. |
| **SUPPLY CHAIN SECURITY AND TRUST** | |
| The Prague Proposals advocate for the responsible behavior of all providers and vendors in the management of their critical supply chains. Especially important is consideration by those operating in critical infrastructure sectors as a breach of those systems can have detrimental effects impacting millions and potentially risking national security. Suppliers are further to be considered based on the influence of their operations by foreign governments including subsidization. Suppliers are evaluated by the extent to which suppliers are subject to, and covered by, rights and obligations consistent with the rule of law, human rights, and democratic values, as well as the robustness of intellectual property protections. | SCS 9001 as a security standard covers the entire product lifecycle including supply chains to ensure that products and services are trustworthy and reliable and that organizations ensure security throughout the supply chain. SCS 9001 requires organizations to collect, analyze and report their security performance based on a defined set of measures. SCS 9001 requires that organizations promote transparency on factors related to the public trust of their business practices and other corporate principles of trust such as providing a recent country score for “Constraints on Government Powers” on the World Justice Project Rule of Law Index, affiliations by key employees including the Board of Directors with political parties or government entities and policies on compliance with international laws and standards pertaining to corrupt practices or bribery. In implementing principles of trust, SCS 9001 utilizes standardized mechanisms so that third parties can confirm an organization’s attestation to each item associated |

| | |
|---|---|
| | with “rule of law, human rights, and democratic values, as well as the robustness of intellectual property protections”. |
| **TRANSPARENCY** | |
| The Prague Proposals advocate for transparency through assessment of ownership, partnership, and corporate governance structures of suppliers of critical components. Suppliers should be able to clearly communicate the security measures taken during the development of their products and services including traceability throughout the technology lifecycle. | SCS 9001 mandates disclosure of corporate organizational structures and governance through the entire supply chain. SCS 9001 addresses supply chain quality and security through mandatory processes covering areas such as Incident Management, Vulnerability Management, Risk Assessment and Mitigation, Provenance, Secure Development, and Open-Source software usage, as examples. SCS 9001 provides for traceability during the complete technology lifecycle with provenance and SBOM requirements. |
| **SECURITY THROUGHOUT THE LIFECYCLE** | |
| The Prague Proposals promote openness, interoperability, robustness, safety and security best practices while ensuring protection of personal data to ensure so that, in conditions of normal use, communications systems function appropriately and do not pose an unreasonable safety risk. Security consideration is required at all stages of the technology lifecycle, including design. | SCS 9001 provides for security by design as a core concept and promotes numerous best practices for protection of systems and users through defined polices such as but not limited to Media Management, Human Resource (HR) Security, Acceptable Use of Assets, Workspace, Access Control Policy, Least Privilege Policy, Asset Management, Mobile Device, Cryptographic Control, Fraudulent/Counterfeit Parts Mitigation, amongst others. |
| **DEMOCRATIC VALUES, HUMAN RIGHTS AND ETHICAL STANDARDS** | |
| The Prague Proposals support an open, interoperable, reliable, and secure internet by promoting a responsible approach to technologies. The Proposals discourage abusive practices in the telecommunication and technology sector inconsistent with recognized human rights principles, including unauthorized surveillance. | SCS 9001 requires that organizations establish methods to effectively manage their supply chain including selection of suppliers. Selection of such suppliers can include those practicing desired human rights principles and SCS 9001 requires that organizations meet all government and regulatory mandates. Finally, SCS 9001 requires attestation to any judgements again the organization for unfair business practices. |
| **PROMOTE R&D AND DIVERSIFICATION** | |
| The Prague Proposals encourage competition to promote vendor diversification and competitiveness and prevent dependence on a small number of suppliers, particularly those considered to be high risk, or a single country in the | Acceptance of and certification to the SCS 9001 standard will provide suppliers a competitive differentiation in becoming preferred suppliers by their customers. The TIA offers various membership options in support of early-stage technology companies. Acceptance of and certification to the SCS 9001 |

| | |
|---|---|
| technology supply chain. Further, like-minded governments are encouraged to collaborate to realize economies of scale. | standard will act as a maturation step for early-stage companies to demonstrate the ability to provide products and services to the demanding ICT industry. |
| **CAPABILITIES DEVELOPMENT AT A STRATEGIC LEVEL** | |
| The Prague Proposals encourage governments to develop capabilities to conduct strategic EDTs assessments, be able to identify and forecast emerging technologies, perform risk assessments to understand the impact of EDTs on national security and take appropriate mitigation measures. | SCS 9001 has been developed with consideration of international government proposed regulations, policies, and executive orders in response to the increasing risk of cyber security attacks and impacts to the supply chains of the ICT industry. SCS 9001 is intended as an international standard and is independent of any product space or vertical. SCS 9001 can be applied as effectively in those EDTs identified within the Prague Proposals as traditional network equipment and software providers within the ICT industry. |
| **RESPONSIBLE TECHNOLOGY TRANSFERS** | |
| The Prague Proposals promote technology flows in an interconnected and global ecosystem. Taken measures should prevent the misuse of technology by malicious actors and could include export controls and screening mechanisms to verify the ownership structure of investors in critical technologies. Efforts should be made to mitigate the risk of a hostile takeover of critical assets and technology that could have a detrimental impact on strategic interests and national security | SCS 9001 is an international standard developed with the cooperation and recommendations of product development organizations, their customers, and government input. SCS 9001 includes best practices that may not prevent malicious acts, but certification to the standard will reduce the potential of cyberattacks and as importantly provides for mitigation and corrective measures if a security incident occurs. SCS 9001 requires the organization to be transparent on numerous corporate principles of trust and these principles are a collection of issues that international governments have identified as being integral in supplier assessment and selection. Additionally, SCS 9001 requires trust principle attestation by the organization in meeting the Transparency Procedures of the Organization for Economic Co-operation and Development Arrangement on Officially Supported Export Credits. |

| Prague Proposal: Telecommunications Supplier Diversity | TIA QuEST Forum SCS 9001™ |
|---|---|
| The Prague Proposals recognizes that industry continues to lead the development of network innovations that support openness and interoperability, but that governments should actively foster an enabling environment for their successful adoption and growth. | SCS 9001 is an international standard that has been heavily influenced by government policy initiatives in response to concerns of the growing thread of supply chain attacks. SCS 9001 will not inhibit innovation, in fact, the organizational maturity resulting in SCS 9001 certification will promote technology innovations. |
| The Prague Proposals encourage consideration of various policy and/or technical measures as well as appropriately targeted commercial incentives to help realize the potential of open and interoperable networks, such as shared R&D initiatives, international pilots and trials, and other activities to stimulate the market. | SCS 9001 certification will provide assurance to users of such products of the high level of security and certainty of how those products were developed in support of rapid deployment of new products and technologies while maintaining security and safety in those deployments. |
| The Prague Proposals suggests governments should seek to collaborate with likeminded countries on these activities, and in addressing policy, technical, or market-based barriers to a more diverse telecoms market ecosystem – while ensuring technologically neutral regulatory environments and fair competition. They should also welcome the emergence of diverse market entrants from likeminded countries whose business practices align with these proposals. | As an international standard, SCS 9001 is ideally positioned to become the de facto standard to ensure secure supply chains for companies operating within the ICT and other industries. |
| The Prague Proposals the subject of this paper, consistent with the 2019 Prague Proposals and the EU Toolbox for 5G Security, encourages governments to ensure that domestic telecoms networks, including open and interoperable ones, are subject to a rigorous evaluation of equipment and infrastructure suppliers that takes into account risk profiles, including the rule of law, the security environment, ethical supplier and transparent financing practices, and adherence to the latest security standards and best practices. | SCS 9001® requires that organizations as part of their certification provide a publicly available registration profile stating their response to a collection of issues that international governments have identified as being integral in supplier assessment and selection. |
| The Prague Proposals highlight the importance of security in the development, deployment, and operation of open and interoperable telecoms solutions through such concerted efforts as global research collaboration, so that the emergence of a wider range of suppliers reinforces resilience across the market. Governments should also support | SCS 9001 promotes numerous best practices in the development of communications solutions and the supply chain leveraged to produce and manufacture such solutions. SCS 9001 does not specifically address goals of universal values, but organizations are free to extend those goals within their supplier selection processes. |

| | |
|---|---|
| approaches to the development of critical and emerging technology that align with universal values, including respect for freedom of expression and privacy. | |
| The Prague Proposals support open, global, industry-led, and inclusive multi-stakeholder approaches for the development of technical standards, including as they relate to telecommunications equipment and services. These international standards will be key enablers to enshrine openness and interoperability in the telecommunications sector, such as through Open Radio Access Networks (Open RAN). | SCS 9001 is an international standard and has been developed through the collaborative efforts of product developers, network operators and government agencies. |
| The Prague Proposals recommend that governments engage in good faith with industry, civil society, and other stakeholders to address obstacles to supplier diversity. This includes creating opportunities for public-private dialogue and stakeholder "buy-in," which are necessary to bring about long-term market evolution. | SCS 9001 was developed through the contributions of suppliers, network operators and government agencies. TIA agrees that ensuring supply chain security and mitigating the potential negative consequences of cyberattacks is the responsibility of all parties. |
| The Prague Proposals encourage network operators, suppliers, and other market actors to consider the expected benefits of utilizing open and interoperable standards-based approaches, so that operators can choose among offerings from multiple suppliers based on performance, pricing, and security. | SCS 9001 is an important international standard that will enable all participants to have assurance in the ability of organizations certified to the standard to deliver high quality products with certainty around their respective supply chains and the security levels of resulting products and services. |
| The Prague Proposals conclude that like other stakeholders, governments should recognize that diversifying telecoms infrastructure markets will require long-term effort and commitment. They should also ensure that public policy efforts evolve to accommodate network advancements, increasing digital connectivity needs, and evolving network risks. | As evidenced by some well publicized security breaches such as the SolarWinds incident, delivering secure products is no longer simply testing the final article to security standards. Suppliers must now focus on securing their supply chains to ensure all components and suppliers of those components are fully vetted. SCS 9001 is a standard focused on exactly that. |

**To learn more about TIA QuEST Forum's SCS 9001 Standard, visit:**

**https://tiaonline.org/what-we-do/scs-9001-supply-chain-security-standard/**