Telecommunications Industry Association
1310 North Courthouse Road, Suite 890
Arlington, VA 22201 | www.tiaonline.org

Telecommunications Industry Association Position Paper

Standards and Guidelines to Enhance Software Supply Chain Security

NIST's request for position papers identified five areas for comment[1] related to standards and guidelines that the Telecommunications Industry Association (TIA) has been doing significant work on for over a year. Specifically, the five areas NIST requested comment on are:

1. Criteria for designating "critical software"
2. Guidelines outlining security measures that shall be applied to the federal government's use of critical software
3. Initial list of secure software development lifecycle standards, best practices, and other guidelines acceptable for the development of software for purchase by the federal government
4. Initial minimum requirements for testing software source code
5. Guidelines for software integrity chains and provenance

TIA, a member-driven and ANSI-accredited ICT industry Standards Developing Organization (SDO), is currently working on two major initiatives which are directed towards addressing these specific areas. TIA is leading an effort in creating an industry-driven, process-based supply chain security standard called SCS 9001.[2] In addition, we are working with key members on Touchstone – guidelines for high quality software development methodologies, including secure software development.

SCS 9001: 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, 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. While the driver for SCS 9001 was the supply chain, many requirements and controls are related to secure software development and management practices. Nine SCS Workgroups have been drafting key requirements for the standard, while also informing and consulting various government agencies. The standard is currently planned for release in 4th quarter 2021.

The standard requires company assets be identified by category, including "Company Critical". Other elements of the standard relevant to NIST's areas of interest include:

- **Cybersecurity Processes** – process requirements for incident management and reporting, risk mitigation, counterfeit parts, legacy network elements, repairs, and maintenance
- **Software and Hardware Identification and Traceability** – process requirements for identifying and validating free and open-source software code, proprietary software and hardware components; as well as updates, versions, origin, and security

[1] NIST call for position papers on standards and guidelines to enhance software supply chain security, (*available at* https://www.nist.gov/news-events/news/2021/05/workshop-and-call-position-papers-standards-and-guidelines-enhance-software).
[2] TIA SCS 9001 Position Paper (*available at* https://www.tiaonline.org/whitepaper).

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

TIA's comments on the FCC NOI on 5G Open Radio Access Networks (Open RAN)[3] identifies the importance of supply chain security for new technologies, and provides multiple examples using real world attacks of how SCS 9001 would help protect the supply chain from vulnerabilities.

SCS 9001 can be used as a standard and guideline for all five areas identified by NIST for enhancing software supply chain security.

Touchstone: TIA's Touchstone effort is a collection of industry best practices for software development methodologies. One very important aspect of Touchstone is cybersecurity. It, too, can be used as a guideline and best practices for ensuring the security of the software development process to enhance the software supply chain security.

Touchstone also addresses the following key cybersecurity elements in creating secure software:

- **Security by design** – architecture and design decisions to be made based on a set of security principles that are tracked throughout the development and release phases; identify security and cryptography needs at the requirements phase
- **Change management** – analyze requirement changes to determine impact on security requirements
- **Procurement** – identify the software procurement needs, including open-source software, to ensure that the software meets the security objective
- **Analyzing overall security architecture** – understand gaps in security control
- **Encryption strategy** – design a strategy to ensure data is encrypted during data flow, data storage, and data usage
- **Code build** – follow secure code practices and guidelines relevant to the technology and environment of the project
- **Code review tools** – use automated tools to identify security vulnerability in the code
- **Component level** – analyze the possibility of security attacks and implement appropriate actions
- **Open Source** – ensure it is the latest version
- **Plugins and Secure Code Agents** – mitigate security vulnerabilities in the design phase
- **Security testing** – utilize multiple techniques such as manual testing, automated security testing, penetration testing.
- **Security audits** – audit the application and analyze results to take corrective action

TIA has put a great deal of effort into standards and guidelines that protect supply chains from vulnerabilities and ensure a secure software development process. We are looking forward to continuing our work with NIST and other industry and government stakeholders to enhance the security of the software supply chain.

[3] TIA Comments on *Promoting the Deployment of 5G Open Radio Access Networks,* Notice of Inquiry, GN Docket No. 21-63 (Filed April 28, 2021) (*available at* https://ecfsapi.fcc.gov/file/104282469110796/2021.04.28_OpenRAN%20NOI_FINAL.pdf).