Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20230

In the Matter of	)	
	)	
Promoting the Deployment of 5G Open	)	
Radio Access Networks	)	GN Docket No. 21-63

COMMENTS OF THE
TELECOMMUNICATIONS INDUSTRY ASSOCIATION

The Telecommunications Industry Association ("TIA")[1] welcomes this opportunity to comment on the matter of Promoting the Deployment of 5G Open Radio Access Networks (Open RAN).[2] As the leading trade association representing the manufacturers and suppliers of communications networks, as an ANSI-accredited standards development organization (SDO), and as the only provider of process-based standards that enable communications providers to monitor and improve their business performance[3], this matter is of vital importance to TIA and its member companies. TIA supports new technologies, including efforts to innovate around network architectures such as Open RAN. We understand that the Open RAN faces similar security challenges as today's RAN and other virtualized architectures[4] and that industry has an important role to play in establishing processes that secure the supply chain for Open RAN and other Information Communications Technology ("ICT") technologies. Also, TIA believes that

[1] TIA is the leading trade association for the information and communications technology industry, representing companies that manufacture or supply the products and services used in global communications across all technology platforms. TIA represents its members on the full range of policy issues affecting the ICT industry and forges consensus on voluntary, industry-based standards.
[2] *Promoting the Deployment of 5G Open Radio Access Networks,* Notice of Inquiry, GN Docket No. 21-63 (Mar. 18, 2021) (NOI).
[3] TIA's TL 9000 Quality Management System (QMS) based on ISO 9001, is the only QMS specifically focused on the communications industry. https://tl9000.org/
[4] O-RAN Alliance Security Task Group, Para. 4, https://www.o-ran.org/blog/2020/10/24/the-o-ran-alliance-security-task-group-tackles-security-challenges-on-all-o-ran-interfaces-and-components

the government should take a technology-neutral approach as it pertains to new technologies. Picking winners and losers among ICT suppliers has the potential to create challenges that could delay the rapid deployment of 5G.

I. OPEN RAN IS THE NATURAL NEXT STEP FOR NETWORK TECHNOLOGY

Openness is a natural evolution of efforts to separate software and hardware functionality, and is already a major part of today's networks. While virtualization of computing systems has been going on for a long time, it began in earnest in the early '00s with the development of new software and hardware that promoted virtualization. In the early '10s software-defined networking brought the separation of software and hardware to networking equipment, e.g., routers and switches. These two technologies have enabled the explosion of data centers and cloud computing, reducing costs and enhancing efficiency. Open RAN is a further implementation of separate software and hardware functionality to bring additional vendor diversity and product offerings to the RAN marketplace. It can introduce new suppliers to the ecosystem, because companies can focus on smaller and more specialized areas of expertise, rather than have to deliver an end-to-end radio network.

New technologies commonly bring changes in threat surfaces that require innovations in security strategies to effectively mitigate risk. Similar considerations also apply to commonly adopted technologies in the ICT marketplace -- change is constant and security is an ongoing process. For example, the rapid deployment of 5G, IoT, smart technologies, and virtualization, by definition, increases the risk of introducing new vulnerabilities with the addition of new devices and new applications. They also bring enormous benefits. Accenture estimates that 5G

will generate up to $1.5 trillion in additional GDP between 2021 and 2025, and will create or transform up to 16 million American jobs.[5]

II. MITIGATING VULNERABILITIES WITH PROCESS-BASED SUPPLY CHAIN STANDARDS

In paragraph 53 of the NOI the FCC asks, "Is there a risk that Open RAN vendors may not yet have the processes in place to address quickly and efficiently possible gaps or bugs that could otherwise be exploited by bad actors?"[6] Ensuring that the proper processes are in place to manage supply chain risk is a problem common to the ICT supply chain, which could reasonably be extended to include the supply of Open RAN compatible equipment. Therefore, Open RAN vendors would benefit, along with other ICT vendors, from adopting ICT standards aimed at addressing this area of risk. In early 2020 TIA and its members recognized that the ICT industry did not have a process-based standard to help ensure the security of the ICT supply chain[7].

In general, there are two types of industry standards: technical standards and process-based standards. Technical standards establish uniform engineering or technical criteria. A consumer can use their mobile phone on any network because there is a technical standard that defines the interface of the phone to the mobile network antenna. Process-based standards are used to control processes to ensure that the end product meets the desired results. Often called a Quality Management System (QMS) it defines and measures an organization's goals, policies,

---

[5] "The Impact of 5G on the United States Economy", Accenture Strategy (Feb. 22, 2021) (*available at* https://www.accenture.com/us-en/insights/high-tech/5g-economic-impact).
[6] NOI at pp. 53.
[7] The term supply chain security is used for both ensuring there is a robust, diverse, and consistent supply chain, as well as, ensuring that the software and hardware providers acquire through their supply chain is verified, secure and free of vulnerabilities. TIA's supply chain security effort addresses the latter.

security practices and interrelated processes to help optimize its performance. QMS measurements can be used to benchmark an organization's performance against others', and as a method to improve that performance. ISO 9001 is the most well-known QMS. Supply chains are a series of interrelated processes and therefore need a process-based standard to ensure security.

Upon realizing the lack of an ICT-focused, process-based standard for supply chain security, TIA and its members created the Supply Chain Security (SCS) Workgroup.[8] It is comprised of equipment providers, software providers, service providers, supply chain experts and security experts. The Workgroup has fast-tracked the creation of a supply chain security standard for the ICT industry, called SCS 9001, which is based on ISO 9001 and TIA's TL 9001 (a QMS for communications networks). It is targeted for release in the third quarter of 2021.

In addition to ISO 9001 and TL 9000, the Workgroup has evaluated over thirty existing process-based standards from multiple industries including transportation, industrial, finance, retail, automotive, aerospace and hospitality. They are taking the relevant elements of each of these standards and then developing new ICT-specific supply chain requirements and controls. They have identified seven additional ICT supply chain security processes; incident management, vulnerability management, risk assessment and mitigation, software usage process, provenance, counterfeit parts, and secure development processes.

The resulting standard will be ICT-focused, global, comprehensive, measurable and verifiable. It will provide the means for service providers and manufacturers to demonstrate and

---

[8] SCS 9001: ICT-Specific Standard for Global Supply Chain Security, April 2021, TIA, https://tiaonline.org/what-we-do/technology-programs/supply-chain-security/scs-9001-ict-specific-standard-for-global-supply-chain-security/

ensure that their supply chains, from end to end, meet the critical benchmarks needed to mitigate risk. As Open RAN applications become a reality, process-based supply chain standards such as SCS 9001 have an important role to play in mitigating the risks that exist in all ICT supply chains so that the benefits of Open RAN can be fully realized.

In early 2021 attackers identified and began exploiting flaws in Microsoft Exchange software.[9] Microsoft quickly released emergency security updates to the software. They patched their cloud-based version of Exchange, but enterprises that had their own servers had to apply the patch themselves. Many did not do so in a timely manner and were vulnerable to attackers for an extended period of time.

TIA's SCS 9001 will require organizations to regularly monitor vulnerability databases for all supplier inputs, such as the NIST Vulnerability Database.[10] It will also require them to measure and track their time to resolve vulnerabilities and submit the measurements to a secure repository managed by TIA. These results will help them improve their processes.[11]

In the example of the Microsoft Exchange attack, a company that implements SCS 9001 would see the vulnerability in the database and quickly act to correct it, thus limiting their exposure from attackers.

---

[9] *At Least 30,000 U.S. Organizations Newly Hacked Via Holes in Microsoft's Email Software,* KrebsonSecurity, Mar. 5, 2021 (*available at* https://krebsonsecurity.com/2021/03/at-least-30000-u-s-organizations-newly-hacked-via-holes-in-microsofts-email-software/).

[10] National Vulnerability Database, National Institute of Standards and Technology, Information Technology Laboratory (*available at* https://nvd.nist.gov/).

[11] Organizations will be able to compare their performance to the industry performance. For example, they will see their performance against Industry Average, Best-in Class and Worst-in-Class performance for other organizations reporting. All data is anonymized, only the reporting company knows their measurement.

Two main components of SCS 9001 are requirements for a secure software development lifecycle (secure SDLC), and software and hardware identification and traceability. Requirements defined in these components will provide significant protection of the organization's products and services, which are even stronger when combined with other components such as incident management, risk assessment and mitigation.

A Secure SDLC requirement will be to "Perform security verification and validation procedures and analyze security-focused results against any established expectations and success criteria." An example of how to do this would be the use of code analysis tools to check not only for software vulnerabilities, but also malware. Known malware has been identified and shared among the security community. Fingerprints have been created and can be identified during the analysis process. These types of processes will be a requirement of SCS 9001 and can help identify vulnerabilities before the code is released.

It is believed that the SolarWinds breach was a bad actor inserting a few lines of code into a dynamic link library file during the software build process. This code allowed an entry point into an enterprise once the software was implemented. A requirement to perform an analysis of the code would likely have helped identify the inserted malware.

The primary requirements for software and hardware identification and traceability will be to "Create a process that assists in the recording of system component origin along with the history of, the changes to, and the recording of who made the changes." Methods to achieve this will include, among other things, requirements for:

- *Provenance/Authenticity* – methods to establish that the software is from the claimed source including the owner, author, release number, build location, license information, version history, etc.
- *Software Bill of Materials (SBOM)*[12] – consistent with NTIA recommendations and shall include supplier name, component name/unique identifier, version, hash, content (open source, free open source, third party), etc.

Provenance and SBOM requirements in SCS 9001, among others, will enable organizations to ensure that components provided by suppliers can be trusted.

III. TECHNOLOGY NEUTRALITY AND DEPLOYMENT

In paragraphs 65-70, the Commission asks a series of questions with respect to whether the FCC should use Universal Service Funds (USF) and appropriations pursuant to the Secure Networks Act to promote the deployment of Open RAN.[13] TIA believes that the FCC should, as outlined in statute, maintain a technology-neutral approach with respect to these funds, and focus on rapid deployment and roll-out. Putting a thumb on the scale and pressuring network operators to use new technologies may have some unintended consequences including:

- *Impacting U.S. national security:* The ICT telecommunications workforce is already limited and constrains the ability of network operators to "rip and replace" equipment

[12] Software Bill of Materials, National Telecommunications and Information Administration (*available at* https://www.ntia.gov/SBOM).
[13] NOI at pp. 65-70.

from untrusted vendors.[14] Pressuring these (mostly rural) network operators to use unfamiliar, new products will slow the removal and replacement of equipment that endangers U.S. national security.

- *Limiting network buildout:* Conditioning the use of federal funds on the use of specific technologies may limit the extent to which these funds can be used to support network build-out. While open interfaces reduce costs to network operators in the long term, there are upfront costs with respect to network integration in the short term that may limit the extent to which these finite pools of funds can be leveraged to expand internet access.

Consistent with past FCC guidance, TIA supports the use of Open RAN to replace equipment from untrusted vendors and to connect underserved communities.[15] TIA also supports the use of vendors with decades of experience building trustworthy, resilient, and secure telecommunications networks throughout the United States. Irrespective of TIA's support of both existing and emerging network architectures, we believe that the government should not support one particular technology over another. These decisions should be left to network operators – who themselves have a strong interest in the long-term benefits of Open RAN – and are in the best position to determine what technologies to use.

---

[14] The FCC Order uses the term "untrustworthy" vendor. In the SCS 9001 standard, there is the concept of verified and unverified suppliers. For U.S. organizations that deploy SCS 9001, entities deemed untrustworthy by the U.S. Government would be considered unverified and treated accordingly.

[15] *See e.g., Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, Second Report and Order, WC Docket No. 18-89 at pp. 202 (Dec. 11, 2020).

IV. CONCLUSION

Open RAN is a natural evolution in network technology, and it has the potential to drive benefits for consumers, network operators, and the environment in the long term. A deliberative, technology-neutral, and deployment-focused approach will ensure that the promise of this technology can be fully realized. TIA looks forward to working with the FCC to help make this happen.

By:

Melissa Newman
Vice President, Government Affairs

Tom McGarry
Vice President, Standards

TELECOMMUNICATIONS INDUSTRY ASSOCIATION
1310 N. Courthouse Road
Suite 890
Arlington, VA 22201
(703) 907-7700

Filed: April 28, 2021