Bobbie Stempfley, Managing Director, CERT Division
Carnegie Mellon University Software Engineering Institute

Hearing on "Legislating to Secure America's Wireless Future"
Before the Subcommittee on Communications and Technology of the
United States House of Representatives Committee on Energy and Commerce

Introduction

Chairman Doyle and Ranking Member Latta, thank you for the opportunity to participate in this hearing on the supply chain risks of the telecommunications industry. I've been a public servant working in IT, focused on the application of information and technology to national security missions for 25 years. I am the Managing Director for the CERT Division of the Carnegie Mellon University Software Engineering Institute (SEI), a Federally Funded Research and Development Center (FFRDC) sponsored by the Department of Defense (DoD). As a leader in cybersecurity, the CERT Division partners with government, industry, non-governmental organizations, and academia to improve the security and resilience of computer systems and networks.

Role of Telecommunication Companies in Security Today and in the Future

The telecommunications sector is a global system, made up of companies, suppliers, and users, that make communication possible. The infrastructure created by the telecoms touches all of us and allows the transmission of data, whether it is video through the airwaves or cables, audio through the phone or Internet, or voice through wires or wireless transmission.

Because the telecom industry is responsible for the flow of information, it is inextricably linked to how we work, play, and live. Communication plays a central role in the fundamental operations of a society—from business to government to families. Whether you need to contact the police, "Google" an address, call your child, or connect citizens to their government, the telecom industry makes it possible. But these connections also have vulnerabilities that create attack surfaces in connected hardware, firmware, or software that must be secured and monitored.

Furthermore, the explosion of edge devices, such as mobile phones, within the telecom infrastructure has only increased the attack surface and therefore the responsibility of the telecoms to protect their users. The role the telecoms play buffering risks from devices they do not control or purchase (such as your home router) makes it all the more important for them to ensure the security of those parts they do buy. Ultimately, the supply chain for the telecommunications industry is vital to achieve security at scale.

Supply Chain Security

What Is Supply Chain Security?

Since the 1990s, the rapid growth of the Internet and its burgeoning role in the transfer of data between telecoms have blurred and blended the boundary between telecom equipment and information technology (IT) hardware. This blending is now defined as information and communications technology (ICT), which emphasizes the role of unified communications and the integration of telecommunications (telephone lines and wireless signals) and computers—as well as the enterprise software, middleware, storage, and audiovisual systems—that allow users to access, store, transmit, and manipulate information.

In the past, when government or business invested in a piece of machinery, appliance, or service, it could more or less expect the item to function as advertised. Checks and balances (such as licenses, warranties, regulations, legal recourse, and supplier reputation) reasonably ensured against defects or service failures. Unfortunately, such controls seem increasingly inadequate when applied to global supply chains for the complex information and communications technology—and technology-based services—that underpin critical capabilities in the telecommunications industry. Concerns about supply chain risk management in ICT include the possibility that counterfeit or maliciously tainted hardware and software might be used by the acquiring organization to its detriment.[1]

All organizations, regardless of sector or mission, have dependencies on others. Organizations are profoundly linked to sources of goods and services not directly under their control, but without access to these critical items, the organizations would fail to achieve their missions. The common challenge now is having confidence in the security practices and processes of entities on which an organization relies when the relationship with those entities may be, at best, an arms-length agreement. Furthermore, we are now faced with a situation where the capabilities of today's software technology environment, the need to outsource, and the interaction between off-the-shelf and open source software products have far outpaced our ability to effectively monitor and manage the risk using traditional methods.[2] With the critical roles that software holds in our operational environments, the impact of fakes, frauds, and malicious activities could be devastating.

We know all organizations have dependencies, but we can no longer rely on formal legal contracts to ensure that suppliers mitigate risk. That approach is ineffective and fails to provide the mechanisms, flexibility, and repeatability needed to manage risks across the entire global supply chain. Effective collection and consumption of cyber threat intelligence requires a managed approach to these dependencies. The veracity of information must be examined and sources evaluated for trustworthiness. An ever-expanding supply chain means that external

[1] Haller, J. "Supply Chain and External Dependencies Risk Management." Software Engineering Institute, Carnegie Mellon University. January 2015.

[2] Alberts, C.; Haller, J.; Wallen, C.; & Woody, C. "Assessing DoD System Acquisition Supply Chain Risk Management." *CrossTalk* (May/June 2017): 4–8.

dependencies must be rigorously measured and strategically managed for an organization to remain resilient. Consequently, today’s evolving landscape requires a comprehensive risk-based approach to managing the supply chain. Its complex nature requires an approach that is sensitive to the hardware, software, and services involved in providing the information and communication capabilities that we rely on. These include addressing:

- Manufacturing and integration supply chains: Responsible for conceptualizing, designing, building, and delivering systems and hardware.
- Service supply chain: Responsible for providing services to acquirers. In a defense context, these include services that vary as widely as data processing and hosting, logistics services, and support for administrative functions.
- Software supply chain: Responsible for producing the software that runs on vital systems.

What Happens Without Supply Chain Security?

Our ICT assets are under constant attack, yet thwarting the active attacker is not something most designers, engineers, developers, or project managers normally consider or have been trained to address. Moreover, most fail to acknowledge the dangers of integrating third-party supplies that may already contain malicious software or hardware. Consequently, no matter how secure you think your systems might be, if your suppliers are not secure, your systems are at risk. Failing to consider the security of your supply chain endangers the daily communications of millions of people, organizations, agencies, corporations, and communities.

Any variety of malicious actors who may have intentions to damage equipment and facilities, steal trade secrets or other sensitive corporate data, alter sensitive information, or cause disruption and devastation can target the telecom infrastructure either from the outside in an attack or from within as a supplier. Therefore, maintaining good supply chain security is paramount to the preservation of integrity and trust in the systems.

We must recognize the telecom infrastructure as the backbone of essential services that depend on connectivity, such as emergency response, utility, transportation, and financial services, among others. Furthermore, telecoms provide vital infrastructure for national security; from natural disaster recovery, to homeland security, to communication of crucial intelligence, to continued military superiority, telecommunications play a pivotal role.[3] The ramifications of an attack anywhere on the telecom infrastructure could spread well beyond the point of origin and have the potential to affect entire nations, businesses, and private citizens.

[3] National Research Council, Division on Engineering and Physical Sciences; Computer Science and Telecommunications Board; & Committee on Telecommunications Research and Development. *Reviewing U.S. Telecommunications Research*. National Academies Press. 2006.

Future Recommendations: How Should Telecoms Secure the Supply Chain?

These bills are a very good first step in supply chain security. As the appropriate entities begin to implement supply chain security, encouraging resilience as a criterion in every stage of development and supply of ICT must continue to be the forward-leaning focus of the software and supply chain assurance efforts within government and industry. Attacks against our supply chains unite acquirers and suppliers in search of scalable means for sharing information about ICT risks that arise through malice or negligence. Suppliers and acquirers need standardized means for conveying information about common issues related to both the hardware and software aspects of ICT, especially regarding non-conforming products that contain counterfeit, tainted, or defective components that can cause subsequent harm.

Fundamentally, the outcomes and risk factors we are seeking to manage are simple, even if the methods to accomplish them are not. (1) Suppliers follow practices that reduce supply chain risks. (2) Products provided by suppliers are acceptably secure. (3) The methods of distribution and/or transmission of the product to the purchaser guard against tampering. And (4) the product or service is used and sustained with acceptable security.

The Acquisition Security Framework and the External Dependencies Management element of the Cyber Resilience Model developed and validated through research at the CERT Division demonstrate that the following practice areas are elements of a mature supply chain risk management effort: relationships, engineering, secure product operations and sustainment, and supply chain technology and infrastructure.

1. Relationships

Supply chain risks are not just managed through technical means; rather they rely on the establishment and sustainment of a relationship between the members of the supply chain. We have moved beyond the day when we were concerned mostly with the identification and integration of “black-box” parts to a concern with more integrated systems with similarly integrated supply chains and dependencies. The ability to maintain production schedules also requires this same relationship management. Through these efforts, companies in the telecommunications sector will receive more insight into the risks and benefits provided by the suppliers.

2. Engineering

Engineering comprises practices to build appropriate cybersecurity controls into systems, operational technologies, and components and minimize the chance of accidentally inserting vulnerabilities. Quality products and services are the result of effective engineering practices and sound test processes AND include distribution and release mechanisms that ensure the released products meet defined requirements, design, and security controls.

An element of this practice area includes understanding the entities within the supply chain. At a basic level this might be a bill of materials, a familiar concept in physical-world manufacturing, such as cars and aviation, which codifies all the ingredients of a product into a list. The bill of materials enables understanding about a product and provides the ability to track defects and changes through the supply chain. Such an inventory can be done with not only hardware components but also software and service components.

The National Telecommunications and Information Administration (NTIA) is over a year into a multistakeholder process for software bills of materials (SBOMs), nearing the end of Phase 1.[4] The CERT Division is co-chairing the Framing Working Group, which is developing and executing an approach for how manufacturers and vendors can communicate useful and actionable information about third-party software components and how enterprises can use this data to inform better security decisions and practices. The goal of this initiative is to foster a market that offers greater transparency to organizations, which can then integrate this data into their risk management approaches. The Framing Working Group has several whitepapers forthcoming.

SBOMs are already being used for license compliance, mainly when commercial vendors include open source components. Just as in the physical world, the supplier of the component, part, or software must define it and provide the SBOM. The NTIA process is examining existing formats, such as the software package data exchange (SPDX) and software identification (SWID) tags. The SBOM has to support nesting, recursion, and relationships (the physical world calls this the multi-level BOM). Lastly, telecom dependencies can be complex, and often key dependencies, like public services (e.g., law enforcement and shared infrastructure) can be overlooked without a proper accounting.

3. Secure Product Operations and Sustainment

Supply chain concerns do not end when the product or service reaches deployment. The telecoms and their suppliers must maintain products and services in their most secure configuration and with the most recent updates. This requires not only patching what the telecoms own, but also involving suppliers to ensure that any impacted fielded capabilities are also operating with the securest versions. This need demonstrates an important use case for the above-mentioned bills of materials, and specifically SBOMs. Telecommunications systems have multi-vendor vulnerabilities and no definitive knowledge about who or what is affected. SBOMs can provide this knowledge. It is not clear what else can.

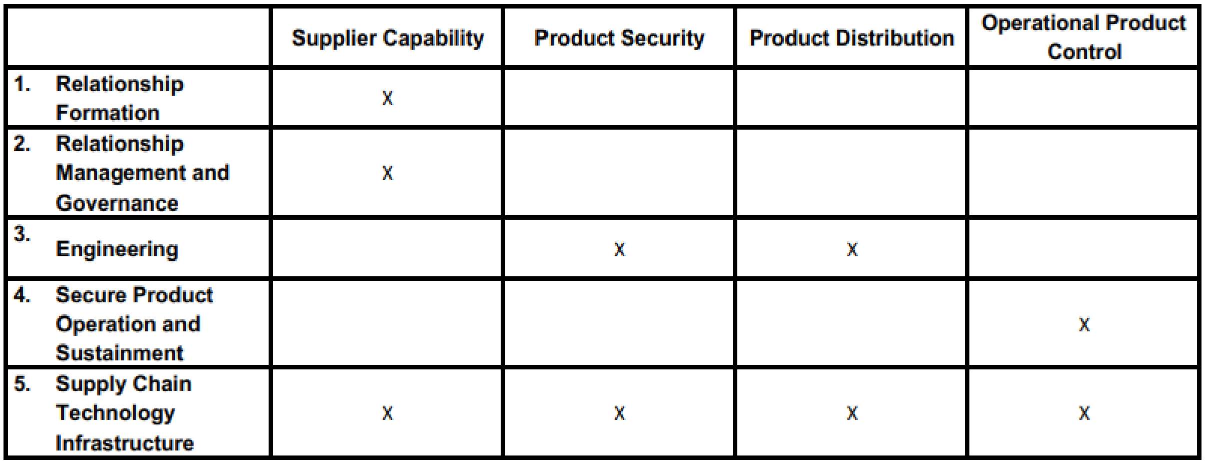
4. Supply Chain Technology and Infrastructure

With the integration of development and supply chains, it is also important to focus on the efforts to secure the technology and infrastructure used to operate the supply chain itself. These efforts range from the need to secure the tools used to develop, integrate, and test software to the efforts to sustain situational awareness requirements for suppliers themselves.

[4] https://www.ntia.doc.gov/SoftwareTransparency

These practice areas cover the range of risk factors that have to be addressed as a part of a mature effort to manage the external dependencies and the supply chain.

Table 1. Mapping of Practice Areas to Risk Factors[5]



	Supplier Capability	Product Security	Product Distribution	Operational Product Control
1. Relationship Formation	X			
2. Relationship Management and Governance	X			
3. Engineering		X	X	
4. Secure Product Operation and Sustainment				X
5. Supply Chain Technology Infrastructure	X	X	X	X

Supply chains can be complex. Communication provider supply chains are often global and support software, hardware, and services that provide vital capabilities for public safety, national security, and general well-being. As private and public functions grow ever more inseparable from the information technology systems that support them, healthy public–private partnerships become even more necessary. To protect this infrastructure against growing and evolving cyber threats requires a layered approach. The government's role in this effort is to share information and encourage enhanced security and resilience while identifying and addressing gaps not filled by the marketplace.

Information pertinent to the supply chain such as vulnerabilities, attack vectors, and supplier security information should be shared along with mitigation plans whenever possible. One good way to collaboratively orchestrate industry and government response to these attacks is through the Common Vulnerabilities and Exposures (CVE) List. The CVE is an extensive listing of publicly known vulnerabilities found after ICT components have been deployed, and it has enabled our operations groups to prioritize, patch, and remediate nearly 60,000 openly reported vulnerabilities. Remediation is a crucial part of the security process, and while our work with the Defense Industrial Base (DIB) highlights the benefits of information sharing, it also emphasizes the need to ensure that everyone at the table, big or small, is able to take appropriate action to mitigate the threats.

Lastly, we should guard against the false choice between security and innovation. It is common to hear that regulations hinder or prevent innovation. Yet regulated industries, such as health care and finance, still practice innovation. Although it is difficult to predict the future impact of telecommunications technologies, services, and applications not yet invented, the technology

[5] Alberts et al., p. 7.

must continue to evolve quickly, and the industry must prevent security technology and concepts from becoming pacing factors in this evolution. Both innovation and security are necessary, and it is possible to have both.