June 2023

COMMUNICATIONS SECURITY, RELIABILITY, AND INTEROPERABILITY COUNCIL VIII

REPORT ON BEST PRACTICES TO IMPROVE SUPPLY CHAIN SECURITY OF INFRASTRUCTURE AND NETWORK MANAGEMENT SYSTEMS

DRAFTED BY

WORKING GROUP 5: MANAGING SOFTWARE & CLOUD SERVICES SUPPLY CHAIN SECURITY FOR COMMUNICATIONS INFRASTRUCTURE

Table of Contents

1 Executive Summary 4
2 Introduction 5
2.1 CSRIC Structure 7
2.2 Working Group 5 Team Members 8
2.3 Subject Matter Expert Contributors 10
3 Objective, Scope, and Methodology 10
3.1 Objective and Scope 10
3.2 Definition and Scope 11
3.3 Methodology 12
3.4 Supply Chain Lifecycle Functions and Infrastructure Component Flow 13
3.5 Vulnerabilities within the Supply Chain Flow 15
3.6 Small Provider Impact and Challenges 15
4 Overview of Current Government and Industry Efforts 16
4.1 Executive Order 14017 on America's Supply Chains 16
4.2 CISA – Defending Against Software Supply Chain Attacks 16
4.3 Executive Order 14028 on Improving the Nation's Cybersecurity 18
4.4 National Cybersecurity Strategy 18
4.5 CISA – Shifting the Balance of Cybersecurity Risk 19
4.6 MITRE Supply Chain Security – System of Trust Framework 21
4.7 ATIS 22
4.8 TIA Supply Chain Security 9001 22
4.9 O-RAN Alliance 23
4.10 Internet Engineering Task Force Supply Chain Integrity, Transparency, and Trust 23
4.11 CISA Cybersecurity Performance Goals (CPGs) 24
5 Hardware Platform Security 24
5.1 Hardware Root of Trust 25
5.2 Secure Storage 26
5.3 Secure Boot 26
5.4 Secure Debug 26
6 Infrastructure and Network Management Systems Supply Chain Threat Vectors 27

6.1 Representative Attacks 27
6.1.1 Hardware Vulnerability – Legacy Platforms 27
6.1.2 Managed CPE Device Events 29
6.1.3 Remote Code Execution (RCE) Exploits 30
6.2 Emerging Threat Vectors 32
6.2.1 Machine Learning/Artificial Intelligence 32
6.2.2 Memory Unsafe Languages 33
6.2.3 Inadequate Zero Trust Implementations 35
6.2.4 Trusted Platform Module Vulnerabilities 36
6.2.5 Continued Operation of End-of-Life Infrastructure for Service Providers 37
6.2.6 Consumer Grade Infrastructure 38
6.2.7 Sourcing Telecommunications Infrastructure from Secondhand Markets 38
7 Summary of Key Findings 40
7.1 Supply Chain Security Specifications and Tools 41
7.2 Government Activities 41
7.3 Zero Trust Principles 42
7.4 HBOMs and SBOMs 42
7.5 Memory Unsafe Languages 42
7.6 ML/AI 43
7.7 Platform Security 43
7.8 Network Management 43
8 Summary of Key Recommendations 44
9 Additional Recommendations for the Commission 48
Appendix A – Resources for Small Providers 51
Appendix B – Glossary 53

1 Executive Summary

As service providers transition to an open virtualized compute environment consisting of infrastructure and network management systems from multiple vendors, the deployment, typically private cloud and/or hybrid-cloud, in the service provider's network is introducing new vulnerabilities and the attack surface is growing. As the Nation emerges from the COVID19 pandemic and recovers from major cyberattacks on various widely used software products, we are now fully realizing the potential impacts and challenges of software supply chain security issues.

The FCC tasked CSRIC VIII, delegated to Working Group 5 (WG5), to produce two reports focused on identifying key security vulnerabilities and recommended best practices to improve communications supply chain security. This first report that CSRIC VIII adopted in September 2022 focused on software supply chain security in this new ecosystem with service providers, cloud service providers, and software vendors to identify recommended best practices to improve communications software supply chain security. This second report focuses on infrastructure and network management system recommendations for service providers, software vendors, and cloud service providers. As discussed in *Section 3*, the report defines the terms "infrastructure" and "network management systems" identifies relevant cyber related events for the two topics. While analyzing publicly published cyber incidences and cyber-attacks relating to infrastructure or network management systems, the report concludes that software supply chain security is very relevant and inseparable from the discussion around infrastructure and network management supply chain security. Understandably, all infrastructure and network management systems contain software which makes the first report relevant for them as well.

CSRIC VIII reviewed several relevant and recent related industry news, security events, and publications. In many of today's compute platforms, the hardware and software components are sourced from global suppliers and open source communities. It is encouraging to see the governmental agencies and several industry bodies, captured in *Section 4*, working independently to address this broad attack vector.

CSRIC VIII has identified some common software supply chain vulnerabilities and corresponding recommendations on how to address those vulnerabilities. The research and analyses are documented in *Section 5* and *Section 6*. Key findings along with identifying key vulnerabilities and associated recommendations are available in *Section 7* and *Section 8*.

The vulnerabilities and threats facing small providers are much the same as for large providers – some attacks target the equipment most commonly used by these providers while supply chain attacks are typically indiscriminate in the size or type of entity they affect. What is different for small providers is the resources they have available to devote to guarding against or recovering from supply chain attacks. The Commission and other federal agencies can help strengthen small providers' supply chain security by offering free cyber resources, such as CISA's vulnerability scanning and funding to hire and train cyber professionals, especially in less populated areas. *Appendix A* identifies some current resources focused on small providers.

2 Introduction

Throughout history, supply chains have always been attacked in a theater of war. Railways, airports, shipping ports, and roadways have been targeted by military leaders to disrupt the enemy's transportation of critical goods needed. These goods could either be to support the war machine or for the humanitarian needs of the civilian population. As seen in the 20th and 21st century battles, fuel pipelines have been targeted as well as the capturing of the raw materials needed by the enemy. Both could end a war in days or weeks versus months or years. As a result, a successful supply chain attack could mean victory or defeat in the theater of war.

Over the past few decades, the world has seen a massive adoption of embedded software in all consumer, industrial, and military sectors. Today's smartphone is 5,000 times faster than the 1985 supercomputer CRAY-2 that was designed by the Department of Defense and Department of Energy.[1] As a result of this explosive growth in compute capabilities, the world has seen almost everything we use contain embedded processors and software. In 1965, Gordon Moore predicted that the number of transistors per silicon chip doubles every year[2] which has not been completely accurate, but it can help us better predict the future regarding the continued evolution of compute capabilities.

In most recent times, nation states and threat actors have realized that they can disrupt an enemy and demoralize a civilian population without the need to use military assets and/or physical detonation devices. For example, instead of using a military airplane or a pack of explosives to disrupt a fuel pipeline, they can now execute a cyber attack on the pipeline's infrastructure or network management systems completely remotely without the need to put their people in harm's way. Since the 1980s, there have been an exponential increase in cyber supply chain attacks.[3] Adversaries' cyber capabilities are evolving and expanding, subjecting the industry to ever-changing tactics, techniques, and procedures (TTPs) to execute these cyber attacks. "The number of documented supply chain attacks involving malicious third-party components has increased 633% over the past year."[4]

In March 2020, Congress passed the Secure and Trusted Communications Act of 2019[5] which became law and establishes a mechanism to prevent communications equipment or services that pose a national security risk from entering the U.S. networks and a program to remove any such

---

[1] Adobe, *Fast-Forward – comparing a 1980s supercomputer to the modern smartphone*, Nov. 8, 2022, https://blog.adobe.com/en/publish/2022/11/08/fast-forward-comparing-1980s-supercomputer-to-modern-smartphone.

[2] Moore's Law, Britannica, 1965, https://www.britannica.com/technology/Moores-law.

[3] Paul Roberts, *A (Partial) History of Software Supply Chain Attacks*, Reversing Labs, June 8, 2022, https://www.reversinglabs.com/blog/a-partial-history-of-software-supply-chain-attacks.

[4] Lucian Constantin, *Supply chain attacks increased over 600% this year and companies are falling behind*, CSO, Oct. 19, 2022, https://www.csoonline.com/article/3677228/supply-chain-attacks-increased-over-600-this-year-and-companies-are-falling-behind.html.

[5] H.R. 4998 – Secure and Trusted Communications Networks Act of 2019, Congress.gov, https://www.congress.gov/bill/116th-congress/house-bill/4998.

equipment or services currently in use. In December 2020, the Commission adopted additional rules and procedures for the implementation of the Act.[6] The Commission took the following steps towards securing our communications networks:

1. Adopted a rule that requires Eligible Telecommunications Carriers (ETCs) to remove and replace covered equipment from their networks.
2. Established a reimbursement program to subsidize smaller carriers to remove and replace covered equipment, once Congress appropriates at least $1.6B.
3. Established procedures and criteria for publishing a list of covered communications equipment or services that pose an unacceptable risk.
4. Prohibits Universal Service Funds (USF) support from being used for such covered equipment or services.
5. Adopted reporting requirements to ensure the Commission is informed about ongoing presence of covered equipment in communications networks.

The Commission plays a critical role in protecting our communications networks. The Commission has continued to update the list of equipment and services that are banned from use within the U.S. communications networks.[7]

In February 2021, President Biden issued Executive Order (EO) 14017 on America's Supply Chains.[8] This EO was primarily focused on the supply chain related issues that started as a result of the COVID pandemic, but the limited supply or unavailability of certain supply chain materials was seen as a national security issue in the broader sense. Beyond the pandemic's impact on certain materials, the Administration issued EO 14028 on Improving the Nation's Cybersecurity in May 2021.[9] Software supply chain security was a key topic of concern in EO 14028, and this triggered many different agencies to start investing time, effort, and energy on software supply chain security. In March 2023, the White House released an updated National Cybersecurity Strategy which includes several Strategic Objectives that have a software supply chain focus.[10] To continue to evolve and strengthen our supply chain and national security, the Commission established the Managing Software & Cloud Services Supply Chain Security for Communications Infrastructure Work Group (WG5) as part of the Communications, Security,

---

[6] *See Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, WC Docket No. 18-89, Second Report and Order, FCC 20-176 (2020).

[7] FCC, List of Equipment and Services Covered By Section 2 of The Secure Networks Act, https://www.fcc.gov/supplychain/coveredlist.

[8] Executive Order 14017, 86 FR 11849, Executive Order on America's Supply Chains (February 24, 2021), https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/24/executive-order-on-americas-supply-chains/ (Executive Order 14017).

[9] Executive Order 14028, 86 FR 26633, Executive Order on Improving the Nation's Cybersecurity (May 12, 2021), https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/ (Executive Order 14028).

[10] National Cybersecurity Strategy (March 1, 2023), https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf (National Cybersecurity Strategy).

Reliability, and Interoperability Council (CSRIC) VIII.[11] In September 2022, CSRIC VIII adopted a report on "Recommended Best Practices to Improve Communications Supply Chain Security" which was primarily focused on the software supply chain.[12] This report is the second installment for this effort, and it will be focused on the communications infrastructure and network management systems (NMS) that are used to operate a communications service provider's (CSP) network. Understandably, all infrastructure and network management systems contain software which makes the first report relevant for them as well.

2.1 CSRIC Structure

CSRIC VIII was established at the direction of the Chairperson of the Federal Communications Commission (FCC) in accordance with the provisions of the Federal Advisory Committee Act, 5 U.S.C. App. 2. The purpose of CSRIC VIII is to provide recommendations to the FCC regarding ways the FCC can strive for security, reliability, and interoperability of communications systems. CSRIC VIII's recommendations will focus on a range of public safety and homeland security-related communications matters. The FCC created informal subcommittees under CSRIC VIII, known as working groups, to address specific tasks. These working groups must report their activities and recommendations to the Council as a whole, and the Council may only report these recommendations, as modified, or ratified, as a whole, to the Chairperson of the FCC.

[11] FCC, CSRIC VIII, https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-council-1.

[12] FCC, CSRIC VIII Report on Recommended Best Practices to Improve Communications Supply Chain Security, September 2022, https://www.fcc.gov/file/23839/download (CSRIC VIII Software Supply Chain Report).

Communications Security, Reliability, and Interoperability Council (CSRIC) VIII					
CSRIC VIII Working Groups					
Working Group 1: 5G Signaling Protocols Security	Working Group 2: Promoting Security, Reliability, and Interoperability of Open Radio Access Network Equipment	Working Group 3: Leveraging Virtualization Technology to Promote Secure, Reliable 5G Networks	Working Group 4: 911 Service Over Wi-Fi	Working Group 5: Managing Software & Cloud Services Supply Chain Security for Communications Infrastructure	Working Group 6: Leveraging Mobile Device Applications and Firmware to Enhance Wireless Emergency Alerts
Co-chairs: Brian Daly, AT&T & Travis Russell, Oracle	Co-chairs: Mike Barnes, Mavenir & George Woodward, RWA	Co-chairs: Micaela Giuhat, Microsoft & John Roese, Dell	Co-chairs: Mary Boyd, Intrado & Mark Reddish, APCO	Co-Chairs: Todd Gibson, T-Mobile & Padma Sudarsan, VMware	Co-chairs: Farrokh Khatibi, Qualcomm & Francisco Sanchez, Harris County Office of HSEM
FCC Liaison: Ahmed Lahjouji	FCC Liaison: Zenji Nakazawa	FCC Liaison: Jeff Goldthorp	FCC Liaison: Rasoul Safavian	FCC Liaison: Zenji Nakazawa	FCC Liaison: James Wiley

Table 1 - Working Group Structure

2.2 Working Group 5 Team Members

Working Group 5 consists of the members listed below.

Name	Company
Rob Alderfer	Charter Communications
Tom Anderson	Alliance for Telecommunications Industry Solutions
Colin Andrews	Telecommunications Industry Association
John-Luc Bakker	BlackBerry Corporation
Donna Bethea-Murphy	Inmarsat
Shirley Bloomfield	NTCA – The Rural Broadband Association
Matt Carothers	Cox Communications
Josh Cech	S&T Telephone Cooperative Association
Dana Golub	Public Broadcasting Service

Name	Company
Anu Jagannath	ANDRO Computational Solutions
Mohammad Khaled	Ericsson
Jason Lish	Lumen Technologies, Inc.
Timothy May	NTIA
Martin McGrath	Nokia
Maureen Mclaughlin	Satellite Industry Association
George Popovich	Motorola Solutions
Travis Reutter	ACA Connects – America's Communications Assoc.
Nasrin Rezai	Verizon Communications
John Roznovsky	Mavenir
Sean Scott	SecuLore Solutions
Paul Steinberg	Motorola Solutions
Jim Stringer	AT&T, Inc.
Richard (Dick) Tenney	Cybersecurity and Infrastructure Security Agency, U.S. Department of Homeland Security
Claire Vishik	Intel
Kelly Williams	National Association of Broadcasters
Henry Young	BSA | The Software Alliance
Padma Sudarsan (Co-Chair)	VMware
Todd Gibson (Co-Chair)	T-Mobile

Table 2 - List of Working Group Members

Alternates for members are listed below.

Name	Company
Reza Arefi	Intel
Tom Breen	Secure Lore Solutions
Mark Carmel	Cybersecurity and Infrastructure Security Agency, U.S. Department of Homeland Security
Cathleen Dwyer	Verizon Communications
Brandon Hinton	Satellite Industry Association

Name	Company
Brian Hurley	ACA Connects
Mike Parsel	T-Mobile
Tamber Ray	NTCA – The Rural Broadband Association
Mike Regan	Telecommunications Industry Association
Mark Roy	Public Broadcasting Service
John Schiel	Lumen Technologies, Inc.
Jason VonBargen	Charter Communications
Timothy Youngblood	T-Mobile

Table 3 - List of Working Group Alternates

2.3 Subject Matter Expert Contributors

The working group heard from several subject matter experts during their research.

Name	Company
Masoud Asadi	Ericsson
Peter Colombo	Cybersecurity and Infrastructure Security Agency, U.S. Department of Homeland Security
Carlos Manzanares	Nokia
Chris Oatway	Verizon
David M. Zendzian	VMware

Table 4 - List of Subject Matter Experts

3 Objective, Scope, and Methodology

3.1 Objective and Scope

The FCC tasked CSRIC VIII, delegated to Working Group 5 (WG5), to identify key security vulnerabilities and recommended best practices to improve communications supply chain security. Building on its September 2022 report that focused on software supply security,[13] in this report, CSRIC VIII focuses on infrastructure and network management system supply chain

[13] FCC, CSRIC VIII Report on Recommended Best Practices to Improve Communications Supply Chain Security, September 2022, https://www.fcc.gov/file/23839/download.

and makes recommendations for service providers, software vendors, and cloud service providers. CSRIC VIII first had to define the terms "infrastructure" and "network management systems" which we capture in the next section. Next, we had to identify relevant cyber related events for the two topics. Surprisingly, there are not many relevant public disclosures or reports relating to infrastructure or network management systems cyber attacks. The first report identified a network management system cyber attack which we used as an example in our software supply chain security discussion. This report identifies a few examples that are relevant and within the purview of the FCC. The report extrapolates on real world events and describes several emerging threats that we see increasing in the future. The report provides a substantive list of vulnerabilities, threats, and risks corresponding recommendations for mitigation.

3.2 Definition and Scope

This report will focus on the communication services infrastructure and network management systems that are within the FCC's purview. These infrastructure and network management systems can be in the cloud and thus are in scope of this report.

- **Infrastructure** includes software-controlled hardware, such as routers, radios, switches, cloud infrastructure, servers, and managed customer premise equipment (CPE). Managed CPE devices can be managed by the CSP and/or cloud providers. Although unmanaged CPE, such as customer-owned equipment and internet of things (IoT) devices, may cause harm to networks, this report does not address this topic. The National Institute of Standards and Technology (NIST) has developed a program that focuses on unmanaged and IoT device vulnerabilities.[14] Likewise, the physical transport media, such as optical and electrical communications cabling, and the materials used to create these components, are out of scope for this report.

- **Network management systems** include applications that enable a CSP to intelligently manage and operate the networks, network segments, and associated network services including the individual devices that are delivering the communication services.

[14] National Institute of Science and Technology, Cybersecurity for IoT Program, https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program.

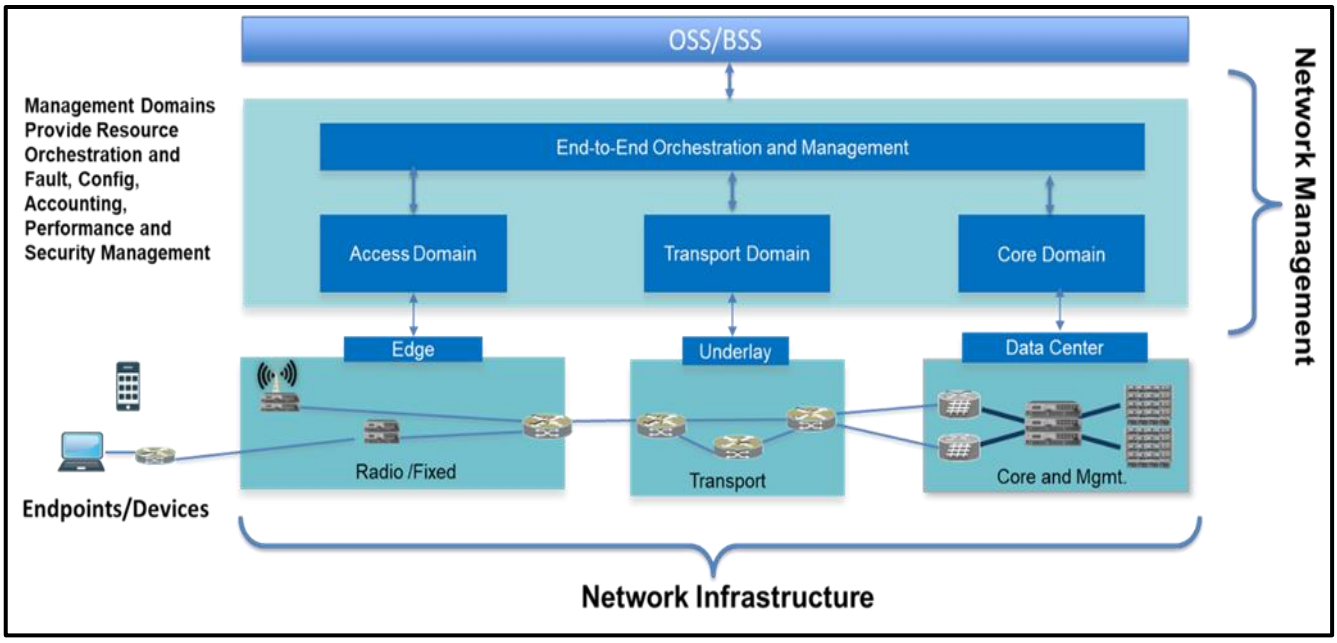

Figure 1: Network Management and Network Infrastructure Scope

Figure 1 shows the scope of network infrastructure and management. Network infrastructure can be a mix of software-controlled hardware devices across different domains - Access, Transport, Core - and can be deployed at different points in the network. Network management consists of a plethora of systems, and can support management and orchestration across Access, Transport, and Core domains with applications that can be deployed in the cloud. VMware defines cloud orchestration as "the process of automating the tasks needed to manage connections and operations of workloads on private and public clouds. Cloud orchestration technologies integrate automated tasks and processes into a workflow to perform specific business functions."[15]

3.3 Methodology

CSRIC VIII's research approach for this report has been to solicit real-world inputs and contributions from WG5 members and invite guest speakers and subject matter experts to share insights during the work group meetings. CSRIC VIII evaluated recent supply chain cyberattacks and emerging threat vectors, industry assessments and guidance, government agency publications and guidance, and specifications produced by standards development organizations (SDOs), captured their analysis, and highlighted exposed vulnerabilities. This enabled CSRIC VIII to identify key findings and recommendations from all the evaluated artifacts with the goal of providing timely, forward looking, sustainable and repeatable supply chain security ecosystem protection for small and large service providers and software and hardware vendors serving the communications infrastructure and network management systems

[15] VMware, *What is Cloud Orchestration?*, https://www.vmware.com/topics/glossary/content/cloud-orchestration.html.

marketplace.

3.4 Supply Chain Lifecycle Functions and Infrastructure Component Flow

The ecosystem surrounding network infrastructure and associated management systems is comprised of a complex set of stakeholder relationships between acquirers, integrators, and suppliers. Depending on certain circumstances, entities can operate in two or more of these roles. These stakeholders manage a complex flow of components that are designed, built, and distributed in a hierarchical manner to create ever more complex systems embedded into systems.

Management of this supply chain can benefit from a high-level model of the supply chain ecosystem illustrating the flow of components through the applicable life cycle functions. Figure 2 below illustrates this life cycle flow. Importantly, the stages shown in this life cycle flow are not intended to convey sequential steps in the supply chain, but rather to illustrate the continuous flow of supply chain functions and processes across the integration and deployment of network infrastructure.

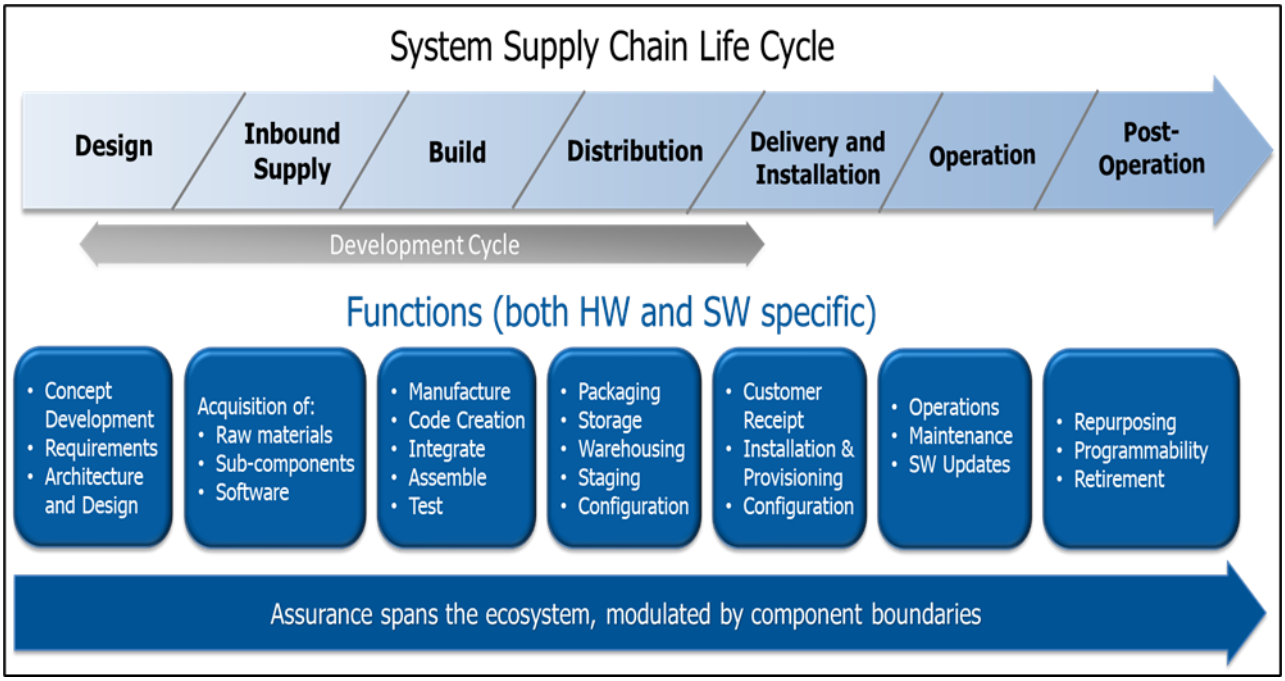

Figure 2: Supply Chain Life Cycle[16]

The supply chain life cycle functions are applicable to both hardware and software components. The identified functions are described as follows:

- *Design* includes concept development, requirements, architecture, and high-level

[16] ATIS, *ATIS Standard: 5G Network Assured Supply Chain - ATIS-I-0000090*, June 2022, https://access.atis.org/apps/group_public/download.php/66150/ATIS-I-0000090.pdf (ATIS Supply Chain Standard).

functional design activities.

- *Inbound Supply* includes the acquisition of raw materials, sub-components, and software necessary for the build process.
- *Build* includes manufacturing (for hardware) and/or coding (for software/firmware) along with the integration, assembly, and test functions.
- *Distribution* includes packaging, storage, warehousing, staging, and initial configuration functions. These functions should follow secure practices.
- *Delivery and Installation* include customer receipt, installation, and associated provisioning, configuration, and network integration.
- *Operation*, from a supply chain perspective, includes inventory management, component replacements or additions, software updates and vulnerability management.
- *Post-Operation* includes functions that may occur once the component is removed from its initial service environment. This may include repurposing, reprogramming, and retirement activities.

Supply chain threats are present for each of the above life cycle functions and should be considered for any supply chain mitigation plan.

Components flowing through the above set of supply chain functions face threats specific to the type of component being considered. Based on vulnerability and threat analysis, for purposes of this report, we categorize components into four basic types: open source software (OSS), proprietary software, software-controlled hardware, and other hardware.

- Open Source Software (OSS) is software that can be accessed, used, modified, and shared by anyone.[17] OSS is often distributed under licenses that comply with the definition of "Open Source" provided by the Open Source Initiative.[18]
- Proprietary software is code which is developed and managed by a software publisher in a closed manner where the source code can only be accessed, used, modified, and shared under the management of the software publisher.
- A software-controlled hardware component typically includes complex processing or compute capabilities along with memory and storage which may be compromised in a way that affects the integrity or behavior of the component while still meeting operational specifications.
- Other hardware has the attribute wherein a compromise of that component generally results in a cyber vulnerability.

[17] *See* NIST, Open Source Code, https://www.nist.gov/system/files/documents/2019/02/19/final_s_6106.01_ver_1.pdf.

[18] Open Source Initiative, https://opensource.org/osd.

3.5 Vulnerabilities within the Supply Chain Flow

Supply chain attacks can generally be separated into two distinct phases:

1. A threat is inserted into a component within the supply chain of an operational system.
2. The vulnerability is then exploited in the operational environment.

As such, there are two classes of mitigation that can be applied: 1) prevention and detection of these vulnerability insertions in the supply chain itself, and 2) operational cybersecurity capabilities specifically designed to mitigate the exploitation of inserted vulnerabilities.

From a hardware or system perspective, supply chain vulnerabilities may exist in either software-controlled hardware or other more passive hardware not directly controlled by software. Vulnerabilities associated with the insertion of malware into software-controlled hardware can enable malicious operational access (e.g., backdoors), denial of service (DoS) attacks, or time bombs that negatively affect operation at a specific time. Vulnerabilities associated with passive / non controlled hardware manifest as attacks on the availability of systems (e.g., a component has been compromised to fail early or in a coordinated fashion). These attacks affect the resilience of the system causing the system to fail at unexpected frequency and in ways from which it may be difficult to recover.

3.6 Small Provider Impact and Challenges

The FCC directed CSRIC VIII to also recommend best practices to mitigate the risks for small communications providers, considering the vulnerabilities that have affected these providers and their capabilities. The World Economic Forum Global Cybersecurity Outlook 2023 Insight Report (WEF Report) echoed the importance of accounting for the supply chains of both small and large companies, noting the interdependence of such companies on one another.[19] In particular, the WEF Report found that "larger firms typically have small and medium organizations in their supply chain and consider them as critical partners. When these critical partners are taken out of action through the technical or financial fallout from a cyber incident, the entire ecosystem, including the larger organizations, is negatively affected."[20]

The 2022 Data Breach Investigations Report by Verizon similarly found that "contrary to what many may think, very small organizations are just as enticing to criminals as large ones, and, in certain ways, maybe even more so."[21] Small communications providers must combat the evolving threat landscape while navigating constraints that can differ from those of a larger provider.

The Office of the National Cyber Director (ONCD) recognized that "de facto responsibility" for navigating the risk of vulnerable technologies has traditionally rested on small businesses,

---

[19] World Economic Forum, *Global Cybersecurity Outlook 2023*, https://initiatives.weforum.org/global-cyber-outlook/home.

[20] *Id.* at 19.

[21] Verizon, *2022 Data Breach Investigations Report*, https://www.verizon.com/business/resources/reports/dbir/.

individuals, and local governments.[22] ONCD further recognized that while these entities play an important role in securing technology, these entities alone cannot and should not shoulder the entire burden. Instead, effective cybersecurity requires cooperation and coordination "across the many public, private, and international stakeholders in the ecosystem."[23]

4 Overview of Current Government and Industry Efforts

The COVID pandemic exposed vulnerabilities in the broader supply chain. At the same time, there were several significant cybersecurity software supply chain attacks that further exacerbated the supply chain issues. Several of these cybersecurity software supply chain attacks were discussed in CSRIC VIII's Report on Recommended Best Practices to Improve Communications Supply Chain Security.[24] As a result of these exposures, the White House took action to shore up the associated vulnerabilities. In turn, several Federal agencies started addressing the software supply chain vulnerabilities aggressively. Parallel to these initiatives, the industry has prioritized their efforts to assist with the mitigation of supply chain security vulnerabilities. This section will discuss several of these key government and industry efforts.

4.1 Executive Order 14017 on America's Supply Chains

Executive Order (EO) 14017 was published on February 24, 2021, and was primarily a response to the supply chain issues as a result of COVID.[25] The EO provided specific directives to various agencies relating to the supply of critical materials such as semiconductors, batteries, critical minerals, rare earth elements, and pharmaceuticals. The lack of an adequate supply of these materials was seriously impacting consumer and manufacturing markets and threatening the national security and economic security of the U.S. Even though this EO did not include any directives relating to the software supply chain domain, the SolarWinds attack was revealed in December 2020 prior to release of this EO.

4.2 CISA – Defending Against Software Supply Chain Attacks

In April 2021, CISA published a software supply chain attack report that introduces guidance on how to defend against such attacks, outlines an information and communications technology (ICT) lifecycle, and provides some example threats for each of their six phases.[26] With respect to infrastructure and NMS supply chain security, CISA's report has several notable recommendations:

---

[22] A Strategic Intent Statement for the Office of the National Cyber Director (October 2021), https://www.whitehouse.gov/wp-content/uploads/2021/10/ONCD-Strategic-Intent.pdf.

[23] *Id.* at 7.

[24] FCC, CSRIC VIII Report on Recommended Best Practices to Improve Communications Supply Chain Security, September 2022, https://www.fcc.gov/file/23839/download.

[25] Executive Order 14017.

[26] CISA, Defending Against Software Supply Chain Attacks, April 2021, https://www.cisa.gov/sites/default/files/publications/defending_against_software_supply_chain_attacks_508_1.pdf.

- **Common Attack Techniques**
  - Hijacking the software updates.
  - Undermining the codesigning process.
  - Compromised open-source code.

- **Actions to Prevent Acquiring Malicious or Vulnerable Software**
  - Validate that the vendor and manufacturer's software development lifecycle (SDLC) uses secure software development practices.
  - Require software inventories via a software bill of materials (SBOM) that articulates the components and other attributes of the delivered software including third-party software components.
  - Organizations should explore opportunities to confirm software and firmware integrity by using common code authentication or other mechanisms. This guidance includes obtaining digital signatures and software/firmware tamper seals.

- **Actions to Mitigate Deployed Malicious or Vulnerable Software**
  - CISA stresses the importance of Vulnerability Management and Configuration Management programs.
  - Focus on the critical data sources and baseline data flows so security anomalies can be detected more easily.
  - Leverage common security controls such as firewalls, network segmentation, and endpoint detection and response (EDR).

- **Actions to Increase Resilience to a Successful Exploit**
  - Explore opportunities to diversify the vendors for critical software in use.
  - Develop and test failover processes that can be used to help an organization recover from a cyber attack.

- **Recommendations for Software Vendors**
  - The development and implementation of a mature SDLC is stressed and should become business as usual for them.
  - Suggest integrating NIST's Secure Software Development Framework (SSDF)[27] into their SDLC.
  - Automate developer and security toolchains in the SDLC.

- **Actions to Prevent Supplying Malicious or Vulnerable Software**
  - CISA suggests that the vendors implement NIST's SSDF to protect the software code and produce well secured software.
  - Vendors should follow the Federal government's approach to high-value assets (HVA) governance program.

[27] NIST, Secure Software Development Framework, https://csrc.nist.gov/Projects/ssdf.

- **Actions to Mitigate Post-Deployment Malicious or Vulnerable Content**
  - Vendors should archive and protect each release of software.
  - Establish an assessment, prioritization, and remediation approach that enables vulnerabilities to be remediated quickly.

4.3 Executive Order 14028 on Improving the Nation's Cybersecurity

The White House published EO 14028 in May 2021 making prevention, detection, assessment, and remediation of cyber incidents a top Biden administration priority and essential to national and economic security.[28] One of the key sections in this EO is "Enhancing Software Supply Chain Security."[29] Some of the relevant statements and directives include:

- Commercial software often lacks transparency, inadequate abilities to resist attacks, and inadequate controls to prevent tampering by malicious actors.
- Vendors need to have secure software development environments.
- Vendors need to be able to generate and/or provide artifacts (e.g., tracks, documentation) that demonstrate their secure software development environment's compliance with this EO.
- Leveraging automated tools to maintain trusted source code supply chains and thus ensuring the integrity of the code.
- Utilization of automated vulnerability scanning tools.
- Providing to purchasers artifacts of the execution of tools and processes to maintain trusted source code supply chains and automated security tools relating to the risks and mitigations; making publicly available summary information on completion of these actions, including a summary description of the risks assessed and mitigated.
- Maintaining accurate up-to-date data and provenance of the software code and components.
  - Providing a SBOM for each product.
  - Participating in a vulnerability disclosure program.
  - Attesting to the integrity and provenance of all open-source software used within the product.

4.4 National Cybersecurity Strategy

In March 2023, the Biden administration issued the "National Cybersecurity Strategy" mapping out five pillars that are targeted at mitigating seven key technology misuses by malicious actors. The strategy touches upon several key areas relevant to this report.[30]

Pillar One defines a number of objectives that are targeted at defending critical infrastructure. Strategy Objective 1.5 calls for the modernization of Federal defenses.[31] This objective includes

[28] Executive Order 14028.

[29] *Id.* at Section 4.

[30] National Cybersecurity Strategy.

[31] *Id.* at 12-13.

the requirement to define new supply chain mitigations that will be implemented to defend critical infrastructure. The expectation is that the supply chain mitigations will be achieved through coordination with NIST to build upon EO 14028, including the SBOM efforts, NIST's SSDF, and related efforts to improve open-source software security.

Pillar Three discusses the need to shape the market forces to drive security and resilience in the broader technology space. Strategic Objective 3.3 outlines the need to shift liability for insecure software products from the customers to the software vendor while providing vendors who use secure development practices a safe harbor.[32] Key relevant points for this report are:

- Many vendors:
  - Ignore best practices for secure software development.
  - Ship products with insecure default configurations.
  - Integrate third-party software of unvetted or unknown provenance.
- Governments must begin to shift liability onto vendors that fail to take responsible precautions to secure their software.
- The responsibility must be placed on the vendors who are the most capable of taking action to prevent bad outcomes. Neither end-users nor the open-source software developer must bear the consequences of insecure software.
- The Administration will work to:
  - Promote the further development and use of SBOMs.
  - Develop a process for identifying and mitigating the risks presented by unsupported software that is widely used or supports critical infrastructure.
- The Federal government will work with the private sector and open-source software community to improve the security of the developed software including the use of memory-safe languages, secure software development frameworks, and security testing tools.

Pillar Five outlines directives to forge international partnerships to pursue shared goals. Strategic Objective 5.5 details a set of activities towards securing the global supply chains for information, communications, and operational technology products and services.[33] The Administration acknowledges the complexity and the interconnectedness of the global supply chain which powers these technology products and services. The objective highlights the risks associated with untrusted suppliers, and mitigation should make the supply chain more transparent, secure, resilient, and trusted. Additionally, the Strategy calls for moving to Secure 5G by working on Open RAN, including activities with the Department of Defense and Department of Commerce, National Telecommunications and Information Administration.[34]

4.5 CISA – Shifting the Balance of Cybersecurity Risk

In April 2023, CISA, NSA, FBI and governmental cyber organizations of Australia, Canada,

[32] *Id*. at 20-21.

[33] *Id*. at 32-33.

[34] *Id*.

United Kingdom, Germany, Netherlands and New Zealand published "Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and –Default."[35] It is intended to advance international conversation and consensus about priorities for vendors as well as for investment and governmental actions to "achieve a future where [digital] technology is safe, secure and resilient by design and default." The report strongly encourages every technology manufacturer to develop and build their products in a way that prevents customers from having to:

- Constantly perform security monitoring.
- Routinely update the vendor's software via patches, etc.
- Perform damage control on the infrastructure and/or platforms to mitigate cyber intrusions.

The publication emphasizes that if vendors "take ownership of improving the security outcomes of their customers," it will shift some of the effort "of staying secure to manufacturers and reduce the chances that customers will fall victim to security incidents" and ensure that the "burden of security should not fall solely on the customer."[36]

Secure-by-Design

The report defines "secure-by-design" as building "… technology products that can reasonably be expected to protect against malicious cyber actors gaining access to devices, data and connected infrastructure." Further, the report states that Secure-by-Design means that "the security of the customer is a core business goal, not just a technical feature. Secure-by-Design products start with that goal before development starts." Secure IT development practices including defense-in-depth are recommended to prevent adversaries from compromising IT systems or gaining unauthorized access to sensitive data. The authoring agencies recommend manufacturers use a tailored threat model in the development stage to address potential threats to a system and account for the system's deployment process. Additionally, they define some tactics that can be used by the vendors to align with this objective:[37]

- Use of memory safe programming languages which aligns with NIST SSDF PW.6.1.
- Incorporate architectural features for memory protections such as those described by Capability Hardware Enhanced RISC Instructions (CHERI).[38]
- Software components including verified commercial software, open-source, and other third-party software should be compliant with SSDF's Secure Software Components.
- Static and Dynamic Application Security Testing (SAST / DAST).
- Software Bill of Materials aligned with SSDF PS.3.2 and PW.4.1.

---

[35] CISA, Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security by Design and Default, Apr. 13, 2023, https://www.cisa.gov/sites/default/files/2023-04/principles_approaches_for_security-by-design-default_508_0.pdf (Shifting the Balance Report).

[36] *Id.* at 5-6.

[37] *Id.* at 8-10.

[38] Capability Hardware Enhanced RISC Instructions, University of Cambridge, https://www.cl.cam.ac.uk/research/security/ctsrd/cheri/.

Secure-by-Default

"Secure-by-default" calls for IT products to be resilient out of the box to prevent exploitation techniques without additional expense or steps, and to make customers aware that deviation from safe defaults increases the likelihood of compromise. The report outlines some tactics that can be used by the vendors to align with this objective:[39]

- Eliminating default passwords.
- Leveraging single sign-on (SSO).
- A software authorization profile.
- Forward-looking security instead of a focus on backwards compatibility.
- Consider delivering an already hardened software product and look at possibly publishing loosening guides instead of hardening guides.
- Consider the user experience consequences of these security configurations.

4.6 MITRE Supply Chain Security – System of Trust Framework

MITRE developed a System of Trust (SoT) Framework that they believe is the foundation for understanding supply chain risks and key to securing "robust and resilient supply chains, trustworthy partners, and trusted components and systems."[40] The SoT Framework seeks to provide a comprehensive, consistent, and repeatable methodology for evaluating suppliers, supplies, and service providers which make up the three main trust aspects of supply chain security.

MITRE defines 14 top-level decisional risk areas under the corresponding three main trust aspects. Additionally, MITRE defines over 200 risk sub-areas by addressing a combination of over 1,200 risk factors and detailed risk management questions. To simplify the adoption and execution of this SoT Framework, MITRE has developed a Risk Model Manager web application.[41] According to MITRE, the web application includes:

- **Body of Knowledge (BoK)** – provides access to predefined profiles and their inventory of yes/no questions used in the SoT assessments.
- **Assessment** – assists in narrowing down SoT content that is more manageable for the supplier, supplies, or service provider in question. The evaluation consists of subject-specific questions to establish the presence or absence of individual aspects of concern and to align with best practices from both government and industry.
- **Scoring** – risks are scored using a set of contextually driven, tailorable, and weighted measurements, which are then used to identify strengths and weaknesses against the applicable risk categories. MITRE claims this will enable the procurer to evaluate suppliers' "trustworthiness" for supplying components or services.
- **Customization** – the tool allows for the customization of the SoT for specific use cases

[39] Shifting the Balance Report at 10-11.

[40] MITRE, Supply Chain Security, System of Trust Framework, https://sot.mitre.org/framework/system_of_trust.html.

[41] MITRE, Risk Model Manager, https://sot.mitre.org/framework/system_of_trust.html#risk_model_manager.

and user environments for the assessment and risk scoring activities.

Figure 3 shows the 14 top-level risk areas which lead to over 200 sub-areas.

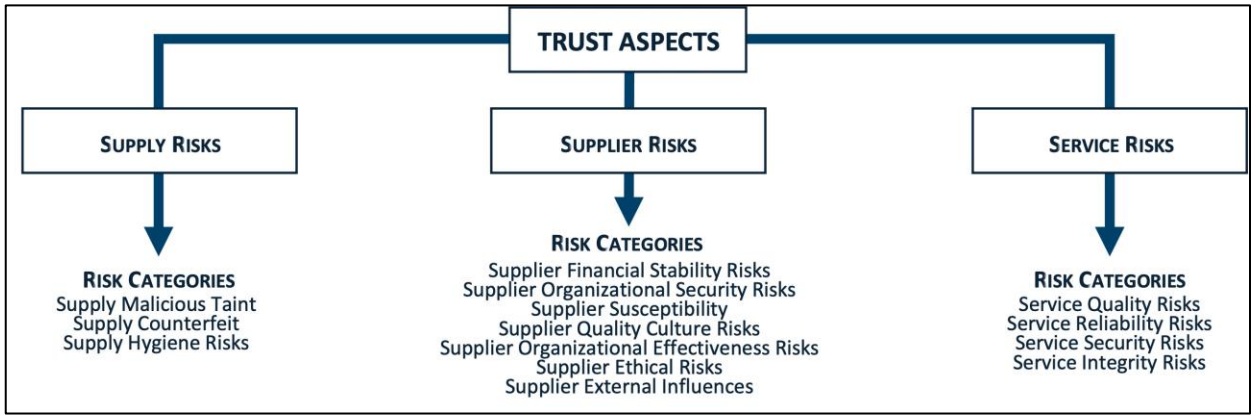

Figure 3: High-Level Depiction of MITRE's SoT Framework

As of preparation of this report, MITRE's Risk Model Manager application is in beta mode. CSRIC was not able to utilize this application in a real world scenario so we collectively cannot make any statements to the effectiveness of the tool or the quality of the outputted assessment scoring.

4.7 ATIS

The ATIS 5G Network Assured Supply Chain Standard provides requirements necessary to operationalize a set of agreed-upon levels of supply chain assurances associated with the deployment and operation of 5G networks.[42] This work is based on a flexible reference model and component flow through the complex 5G supply chain to identify a complete set of controls that can mitigate the identified threats and associated attacks given a specific level of assurance. Attack classes are identified by using defined attributes. These attributes represent a defining quality of an asset (hardware component, module, system, software) and consequently reflects the asset's attackable characteristics.

4.8 TIA Supply Chain Security 9001

The Telecommunications Industry Association (TIA) is a global SDO that has been operating for over 80 years. TIA has produced the Supply Chain Security 9001 Cyber and Supply Chain Management System (SCS 9001) for the ICT industry to help address problems of cyber and supply chain security.[43] TIA believes that SCS 9001 can be leveraged by network operators of all types in their own operations as well as to provide assurance that their upstream vendors can

[42] *See* ATIS Supply Chain Standard at 18-24.

[43] TIA, Supply Chain Security (SCS) 9001, https://tiaonline.org/what-we-do/scs-9001-supply-chain-security-standard/.

be trusted as providers of inherently secure products and services.

SCS 9001 recognizes the blurring line between Information Technology, Operational Technology, modern network architecture and the increased emphasis of using a secure software development lifecycle process leveraging development, security, and operations (DevSecOps) practices. There can be no distinction between network elements that carry and store user data and those elements used to manage the network. All are subject to exploitation.

SCS 9001 can be used for self-assessment or be the basis of independent certification. The standard provides requirements and controls to provide a higher level of assurance that network elements of all types have been developed by organizations that embrace intrinsic operational security practices including a product development process that includes security considerations across the entire product lifecycle.

4.9 O-RAN Alliance

The O-RAN Alliance Work Group WG 11 (OAWG 11) has been focused on addressing security requirements for telco deployments including cloud-based deployments.[44] As the number of components in a disaggregated 5G system (5GS) increase, so does the size and complexity of the supply chain of such a system. The group is also including supply chain related "Security Threat Modeling and Remediation" and adding requirements in the specifications that will mitigate the threats.[45]

In addition to OAWG 11, O-RAN has a "next Generation Research Group" (nGRG) that is looking at research topics on future technologies and supply chain threats.[46] Some forward-looking recommendations may come out of this group. This is a space to watch for new technology solutions to address concerns we have raised in this report.

4.10 Internet Engineering Task Force Supply Chain Integrity, Transparency, and Trust

The Internet Engineering Task Force (IETF) Supply Chain Integrity, Transparency, and Trust (SCITT) work group is chartered to define a set of interoperable building blocks that will allow implementers to build integrity and accountability into software supply chain systems to help assure trustworthy operation.[47] Its goal is "to standardize the technical flows for providing information about a software supply chain, which also includes firmware, and covering the essential building blocks that make up the architecture."[48] The work group will reuse existing

---

[44] *See* O-RAN Alliance, Specifications, https://orandownloadsweb.azurewebsites.net.

[45] O-RAN Alliance, Security Threat Modeling and Remediation Analysis 5.0, O-RAN Alliance Specifications, https://orandownloadsweb.azurewebsites.net/specifications.

[46] Juan Pedro Tomas, *O-RAN Alliance launches research group to focus on 6G*, RCR Wireless News, June 30, 2022, https://www.rcrwireless.com/20220630/open_ran/o-ran-alliance-launches-research-group-focus-6g.

[47] IETF, Supply Chain Integrity, Transparency, and Trust (SCITT), https://datatracker.ietf.org/group/scitt/about/.

[48] *Id*.

IETF working groups, such as Concise Binary Object Representation (CBOR) Object Signing and Encryption (COSE)[49] and remote attestation procedures (RATS),[50] and coordinate with the various standards bodies, such as OpenSSF, W3C, and ISO. SCITT has produced a number of software supply chain use cases. By the end of 2023, they plan to finalize the use cases, security objectives, concise threat modeling document, and the architecture and terminology document. By June of 2024, they plan to submit an HTTP-based representational state transfer (REST)[51] application programming interface (API)[52] for Request-Response interactions and a Countersigning Format for Claim Registration. This work is quite novel in approach and hopefully will help bring a unified strategy and standard globally.

4.11 CISA Cybersecurity Performance Goals (CPGs)

The National Cybersecurity Strategy announced by the White House on March 2, 2023, referred to the Cybersecurity and Infrastructure Security Agency's (CISA) Cybersecurity Performance Goals (CPGs) as an important tool to provide cybersecurity guidance to critical infrastructure entities.[53] The CPGs identify a baseline set of cybersecurity practices, which include examples of ways to implement the recommendations.[54] Most relevant to this report, the CPGs contain a section on supply chain security, which describes actions entities can take to enhance their network security.[55] While the CPGs are designed for all sectors and companies of all sizes, CISA anticipates that small entities may benefit the most from the CPGs because they include a "recommended action" for each goal. These "recommended actions" can provide helpful first steps for small providers that are not staffed with trained and experienced cybersecurity personnel.

5 Hardware Platform Security

Platform security is related to the security of the hardware and is the foundation of the security capabilities in a product. The main building blocks for platform security can be listed as Root of Trust, Secure Storage, Secure Boot, and Secure Debug. These building blocks are briefly described below. Moreover, a flexible and robust platform security solution requires a solid and futureproof key management service utilizing up to date hardware crypto engines and true random number generator (TRNG) engine. Hardware platform security is critical for both infrastructure and NMS supply chain security. NIST discusses this topic in their document

---

[49] IETF, Concise Binary Object Representation (CBOR) Object Signing and Encryption, RFC 8152, https://datatracker.ietf.org/group/cose/about/.

[50] Remote Attestation Procedures (RATS), IETF, https://datatracker.ietf.org/wg/rats/about/.

[51] REST, Wikipedia, https://en.wikipedia.org/wiki/Representational_state_transfer.

[52] API, Wikipedia, https://en.wikipedia.org/wiki/API.

[53] National Cybersecurity Strategy at 8.

[54] CISA, Cross-Sector Cybersecurity Performance Goals, March 2023, https://www.cisa.gov/cross-sector-cybersecurity-performance-goals.

[55] *Id*. at 9-10, 19.

"NIST IR 8320 Hardware-Enabled Security: Enabling a Layered Approach to Platform Security for Cloud and Edge Computing Use Cases."[56]

5.1 Hardware Root of Trust

Component authenticity is an important attribute when considering supply chain threats. As such, it is useful to leverage techniques that can securely link back to a component's provenance to verify the authenticity and integrity of that component. The use of a Hardware Root of Trust (HRoT) is one such technique. HRoT is the main enabler of the security features in products. It provides a secure means to store cryptographic secrets that are critical to the system security, trusted cryptographic functions, and ability to extend trust to other entities via these secrets and functions. Important properties of the HRoT component include:

- Hardware based hence extra resistant to attacks and can be permanent in the field.
- Limiting access to cryptographic secrets based on need and function.
- Secrets can be uniquely programmed on each system so if cryptographic secrets are compromised, only that system is affected.
- Hardware accelerated cryptographic (encryption/decryption) services.

An HRoT must be inherently trusted, therefore, it must be secure-by-design providing a foundation on which all secure operations of a computing system depend. It contains secured and protected keys and cryptographic functions to enable secure platform identification (using unique keys verified via the protected cryptographic functions). Ensuring the quality of keys (key structure, key redundancy, crypto used, key length, and key expiration) is important. A key hierarchy structure (e.g., primary key and secondary key) should be used. Keys should be redundant (e.g., several primary keys). Key renewal and revocation mechanisms should be utilized and a solid and futureproof key management service utilizing up to date Hardware Crypto engines such as RSA, ECDSA, and SHA, and TRNG is needed. In addition, an HRoT can be used for software and firmware attestation. Firmware can then be used to verify software-controlled aspects of the platform. HRoT implementation may also include a measurement function to enable information about the software, hardware, and configuration of a system to be collected and digested. These capabilities can be used to increase the level of assurance associated with component authenticity and integrity.

An HRoT can be implemented using a variety of technologies. NISTIR 8320 discusses the use of a hardware security module (HSM) to store measurement data to be attested at a later point in time. Specifically, an HSM is "a physical computing device that safeguards and manages cryptographic keys and provides cryptographic processing."[57] An HSM typically hosts cryptographic operations such as encryption, decryption, and signature generation/verification.

---

[56] NIST, Hardware-Enabled Security: Enabling a Layered Approach to Platform Security for Cloud and Edge Computing Use Cases - NIST IR 8320, May 2022, https://nvlpubs.nist.gov/nistpubs/ir/2022/Nist.IR.8320.pdf.

[57] NIST, Hardware-Enabled Security: Enabling a Layered Approach to Platform Security for Cloud and Edge Computing Use Cases - NISTIR 8320, https://csrc.nist.gov/publications/detail/nistir/8320/final.

Many implementations provide hardware-accelerated mechanisms for cryptographic operations.

Similarly, NISTIR 8320 also describes the trusted platform module (TPM) as a special type of HSM that can generate cryptographic keys and protect small amounts of sensitive information, such as passwords, cryptographic keys, and cryptographic hash measurements. The TPM can be integrated with server platforms, client devices, and other products.

In addition, many applications utilize a trusted execution environment (TEE) to create an HRoT. A TEE is an isolated execution environment providing security features such as isolated execution to enable higher levels of application integrity and confidentiality.

5.2 Secure Storage

Secure Storage is a service in hardware to store data objects securely in a non-volatile fashion on the circuit board. Secure Storage handles any given data object that is subject to protection, without any need to have knowledge about the actual content or where the data object is finally stored on the circuit board. The storage service is a circuit board unique service which applies storage keys that are known only locally on the circuit board and cannot be accessed by any other circuit boards.

5.3 Secure Boot

To enable trustworthy computing in trustworthy products, the processing on the product must be brought up in a secure state. Secure Boot is the basic feature that provides this security and trustworthiness. It is used to ensure the authenticity and integrity of the different boot stages that are loaded before the OS and application software are loaded. The Secure Boot starts up the hardware in stages and protects the boot process up to the OS stage where signed software continues to protect the start-up of the application layer. All boot stages are digitally signed with independent secret keys and are not allowed to start unless the signatures are authenticated. By supporting the anti-rollback function, the feature also ensures that older, invalidated versions of the software are prohibited from being loaded and started.

5.4 Secure Debug

Secure Debug is one of the most important platform security requirements, as the debug port is a potential open door for attackers because it provides full access to code and data. Therefore, Joint Test Action Group (JTAG) Debug port is one of the most common hardware interfaces used for advanced hardware troubleshooting.[58] Access to debug ports should be locked to maintain operational security and a secure unlock should be supported when access is required by an authorized entity. The Secure Debug basic feature ensures that only parties in possession of authentic debug firmware are allowed to access board resources through the JTAG debug port.

[58] JTAG is an industry standard for verifying designs and testing printed circuit boards after manufacture, https://en.wikipedia.org/wiki/JTAG.

In summary, security needs to be built in the hardware platforms from the start. This includes security built in the silicon with a chain of trust that goes all the way up to the application layer to ensure that only authorized and digitally signed software can be loaded into that hardware. Hardware platform security is the foundation of all secure operations in the platform that protects the data in rest, in transit, and in use. Hardware-based secure storage is needed to prevent unauthorized access to the data. Storage Root Keys are used to protect vendor and user sensitive data and key material. Only vendor signed software is allowed to prevent manipulation with software and the possibility to get hold of keys.

6 Infrastructure and Network Management Systems Supply Chain Threat Vectors

CSRIC VIII used published cyber attacks that pertain to infrastructure and NMS, as defined in Section 3.2 above and within the FCC purview. This narrowed scope resulted in a limited number of applicable cyber security events which are captured in Section 6.1 - Representative Attacks. As a result, CSRIC VIII developed a list of emerging threat vectors, Section 6.2 - Emerging Threat Vectors, which is based upon the Work Group's industry knowledge and experience.

6.1 Representative Attacks

6.1.1 Hardware Vulnerability – Legacy Platforms

In early 2022, researchers reported that beginning in 2020, Chinese state-sponsored threat activity groups had been targeting India's critical infrastructure, including its energy sector and the industrial control systems (ICS) used to operate and maintain the electrical grid.[59] In one instance, the intrusions targeted seven Indian State Load Dispatch Centers responsible for carrying out real-time operations for grid control and electricity dispatch within the states. The attacks extended to a national emergency response system and an Indian subsidiary of a multinational logistics company.

How the Attack was Carried Out: In follow-on research, the threat vector was assessed to be the Boa web server commonly used to access settings, management consoles, and sign-in screens.[60] Although its product developer discontinued it in 2005, Boa continues to be included in a range of software developer kits (SDKs), which contain essential functions that operate system on chip (SOC) implemented in microchips that IoT device developers use in their design of critical components for ICS. Popular SDKs are used in SOCs provided to companies that manufacture gateway devices, including routers, access points, and repeaters.

---

[59] Recorded Future, *Continued Targeting of Indian Power Grid Assets by Chinese State-Sponsored Activity Group*, Apr. 6, 2022, https://go.recordedfuture.com/hubfs/reports/ta-2022-0406.pdf.

[60] Microsoft, *Vulnerable SDK Components Lead to Supply Chain Risks in IoT and OT Environments*, Nov. 22, 2022, https://www.microsoft.com/en-us/security/blog/2022/11/22/vulnerable-sdk-components-lead-to-supply-chain-risks-in-iot-and-ot-environments/. In its report, Microsoft identified over 1 million Internet-exposed Boa server components around the world.

Impact of the Attack: Boa web servers and SDKs have a number of known vulnerabilities and represent a persistent risk across the IoT supply chain. Nevertheless, they remain in use and thus legacy server platforms such as Boa represent a significant attack vector in critical infrastructure networks. Figure 4 below shows an example of the permeation of the vulnerability through the supply chain. Without developers managing the Boa web server, the product developer warned that its known vulnerabilities could allow attackers to silently gain access to networks by collecting information from files. Further, those affected like the Indian power companies may be unaware that their devices run services using the discontinued Boa web server, and that firmware updates and downstream patches do not address its known vulnerabilities.[61] The popularity of the Boa web server displays the potential exposure risk of an insecure supply chain. In this instance, updating the firmware of IoT devices does not always patch SDKs or specific SOC components and end users have limited visibility into components and whether they can be updated.

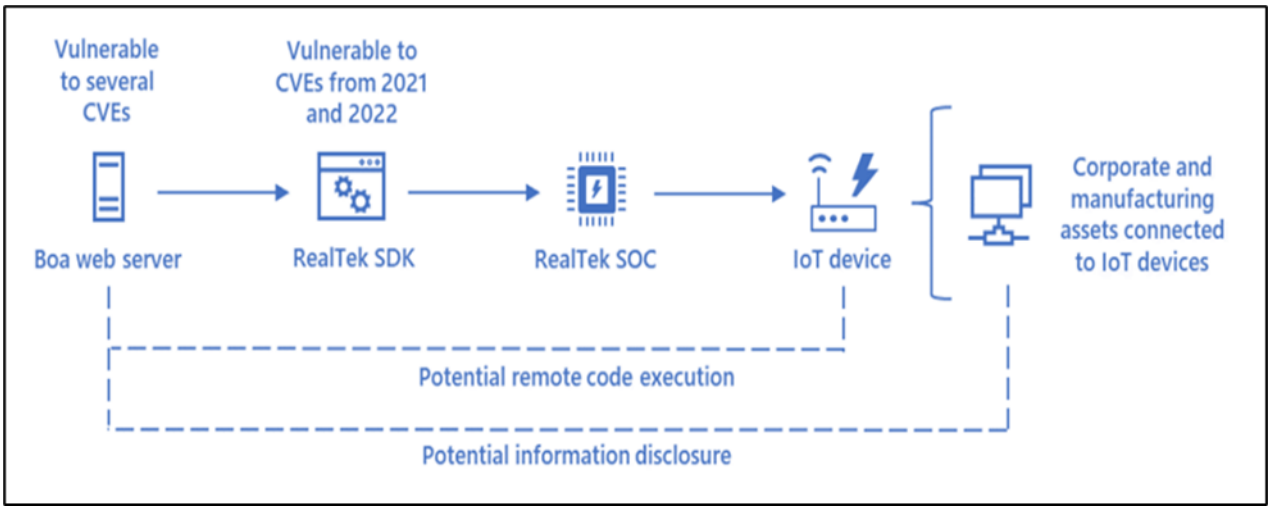

Figure 4 – IoT Supply Chain Vulnerability[62]

Mitigation Recommendations: In its assessment, Microsoft offered a number of best practice guidelines for their networks, including:[63]

- Patch vulnerable devices whenever possible to reduce exposure risks across the organization.
- Use device discovery and classification to identify devices with vulnerable components by enabling vulnerability assessments, which identifies unpatched devices in organizational networks; set workflows for initiating appropriate patch processes.
- Extend vulnerability and risk detection beyond the firewall to identify Internet-exposed

[61] *Id.*

[62] *Id.*

[63] *Id.*

infrastructure running legacy web server components.

- Reduce the attack surface by eliminating unnecessary Internet connections to IoT devices in the network. Apply network segmentation to prevent an attacker from moving laterally and compromising assets after intrusion. In particular, IoT and critical device networks should be isolated with firewalls.
- Configure detection rules to identify malicious activity.
- Adopt comprehensive IoT and operational technology solution to monitor devices, respond to threats, and increase visibility in order to detect and alert when IoT devices with legacy server such as Boa are used as an entry point to a network.

6.1.2 Managed CPE Device Events

The KA-SAT network provides broadband communications internet service to more than 30,000 satellite terminals across Europe. The service is used within a variety of industries including consumer, industrial and government applications.

On February 24, 2022, reports of lost connections began to surface, starting with reports from a major German energy company that had lost remote monitoring capabilities over 5,800 wind turbines. Some KA-SAT services were compromised due to a "cyber event" that impacted around half of the previously active modems within Ukraine, and a substantial number of additional modems in other parts of Europe.

The assessment of the event which follows is taken from the operator and subsequent guidance provided by CISA and the FBI.[64]

How the Attack was Carried Out: Investigation identified a ground-based network intrusion by an attacker exploiting a misconfiguration in a VPN appliance to gain remote access to the trusted management segment of the KA-SAT network. The attacker used this network access to execute legitimate, targeted management commands on a large number of residential modems simultaneously.

Additionally, these commands overwrote key data in flash memory on the modems, rendering the modems unable to return to the network, but not permanently unusable. No modems were permanently 'bricked' —rather they were rendered inoperable and were incapable of being remotely recovered. In addition, large volumes of traffic intended to disrupt the network was also observed, however, the network stabilized within a few hours while preserving service for the majority of customers served.

Impacts of the Attack: Outside of the loss of service to users, recovery time was lengthy for some users. While there are multiple unconfirmed reports that suggest that all connected modems' firmware was wiped, the attack only affected modems in one of two logical network segments, unrelated to which version of firmware was in the affected modems. A review of impacted modems confirmed no anomalies or impacts to the devices and discovered no evidence of a compromise to modem software, firmware images or supply-chain interference. The

[64] CISA, *Strengthening Cybersecurity of SATCOM Network Providers and Customers*, May 10, 2022, https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-076a.

modems could be fully restored via a factory reset.[65] Given that over the air recovery was not possible, tens of thousands of replacement modems were shipped to distributors to provide to impacted customers. This expedited a logistical response for restoration of service to impacted customers relative to refurbishing each modem.

Mitigation Recommendations: The attack leveraged IT policies that were vulnerable in protecting an internet connected VPN appliance which provided access to the operator's trusted management network. The modem attack would have been prevented if not for that failure, but might have been mitigated by practices such as:

- Applying stringent access controls to critical management networks and network services including multi-factor authentication and password rotations.
- Avoiding the use of shared accounts which may have shared knowledge of credentials.
- Applying the principle of least privileged access.
- Monitoring device logs for anomalous activity.
- Implementing improved monitoring at ingress and egress points of SATCOM networks and at the terrestrial network interconnection boundary.
- Ensuring robust device update and patching capabilities, never require physical access to a device for recovery (unless there is physical damage to the device).
- Providing the ability to audit system configuration changes and flag anomalous activities.
- Monitoring all logs for suspicious activity.
- Setting a baseline for normal network traffic and monitoring for aberrations.
- Reviewing and ensuring the effectiveness of incident response and recovery plans.

6.1.3 Remote Code Execution (RCE) Exploits

Remote code execution (RCE) is when an attacker accesses a target computing device and makes changes remotely, no matter where the device is located. RCE takes advantage of vulnerabilities in the implementation of a system component, such as the ability to overflow heaps and stacks, to load and execute malicious code *at runtime* and with privileges that allow it to take over system control.

6.1.3.1 Federal Agency Hacked – Attackers Exploited Webserver Vulnerability

In late 2022 and early 2023, multiple hacker groups initiated an attack against a federal civilian executive branch (FCEB) agency to exploit a .NET deserialization vulnerability in an instance of

[65] *See, e.g.*, Viasat, *KA-SAT Network Cyber Attack Overview*, Mar. 30, 2022, https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview; Rachel Jewett, *Viasat Details KA-SAT Cyberattack that Affected Thousands of Modems in Ukraine*, Via Satellite, Mar. 30, 2022, https://www.satellitetoday.com/cybersecurity/2022/03/30/viasat-details-ka-sat-cyberattack-that-affected-thousands-of-modems-in-ukraine/.

Telerik user interface (UI) for ASP.NET AJAX running on the agency's Internet Information Services (IIS) webserver.[66]

How the Attack was Carried Out: The successful exploitation of the vulnerability let attackers execute an arbitrary code remotely on the agency network where the vulnerable Telerik UI is presented in the IIS webserver. CISA observed that the threat actor XE Group started their system enumeration beginning in August 2022 and were able to upload malicious dynamic link library (DLL) files to the C:\Windows\Temp\ directory, achieve remote code execution, and then execute the DLL files via the w3wp.exe process. According to CISA, this exploit, which results in interactive access with the web server, enabled the threat actors to successfully execute remote code on the vulnerable web server. Though the agency's vulnerability scanner had the appropriate plugin for the vulnerability, it failed to detect the vulnerability due to the Telerik UI software being installed in a file path it does not typically scan. This may be the case for many software installations, as file paths widely vary depending on the organization and installation method.

Impact of the Attack: When the dynamic link library (DLL) files are loaded, the files can read, create, and delete files. If the DLL contains a hardcoded IP address, status messages will be sent to the IP. One DLL file will attempt to collect the target system's Transmission Control Protocol (TCP) connection table, and exfiltrate it to a remote Command and Control server (C2). Other files drop and decode a reverse shell utility that can send and receive data and commands. In addition, the files drop and decode an Active Server Pages (ASPX) web shell. Lastly, two DLL files are capable of loading and executing payloads.[67]

Mitigation Recommendations: To minimize the threat of other attacks targeting this vulnerability, CISA, the FBI, and the Multi-State Information Sharing and Analysis Center (MS-ISAC) recommend several mitigation measures:

- After proper testing of all Telerik UI ASP.NET AJAX instances, upgrade all instances to the latest version.
- Using Microsoft IIS and remote PowerShell, monitor and analyze activity logs generated by these servers.
- The permissions that can be granted to a service account should be kept at a minimum in order to run the service.
- Ensure that vulnerability scanners are configured in such a way as to cover a comprehensive range of devices and locations.
- In order to separate network segments according to a user's role and function, network segmentation should be implemented.

---

[66] CISA, Threat Actors Exploited Progress Telerik Vulnerability in U.S. Government IIS Server, Mar. 15, 2023, https://www.cisa.gov/sites/default/files/2023-03/aa23-074a-threat-actors-exploit-telerik-vulnerability-in-us-government-iis-server_1.pdf.

[67] CISA, MAR-10413062-1.v1 Telerik Vulnerability in U.S. Government IIS Server, Mar. 15, 2023, https://www.cisa.gov/news-events/analysis-reports/ar23-074a.

6.2 Emerging Threat Vectors

6.2.1 Machine Learning/Artificial Intelligence

Machine learning (ML) and artificial intelligence (AI) are used to automate processes, optimize network performance, and improve the overall customer experience. However, ML/AI can introduce cyber vulnerabilities that must be addressed to maintain network security and reliability. A general scenario would involve a network management system (NMS) vendor that delivers a solution to a CSP that leverages ML/AI to allow the solution to work in semi-autonomous mode. A vulnerability arises if the NMS vendor does not adequately secure the ML data sets and a threat actor injects spurious data skewing the outcome and making it a potential attack vector. If the NMS solution is within the perimeter of CSP's network or has implicit trust with critical infrastructure, then the threat actor could exploit this inadequate security to disrupt the communication services.

Machine Learning and Artificial Intelligence present distinct challenges for next generation networks. Today, 5G networks, which promise higher data rates, lower latency, and improved connectivity, are leveraging ML/AI to improve performance. For example, ML/AI is used in 5G network automation to govern the provision, configuration, management, and optimization of network resources.[68] It enables network operators to reduce manual intervention, increase efficiency, and improve security quality. Nevertheless, ML/AI is subject to certain cyber vulnerabilities.[69] Threat vectors include:

- Data Poisoning: An initial type of ML/AI attack is data poisoning.[70] In this scenario, ML algorithms are trained on large datasets to learn patterns and make predictions. However, threat actors could manipulate these datasets by injecting malicious data into the training data to bias the ML model. These attacks can cause the ML model to make incorrect predictions and compromise network security.
- Model Stealing: Model stealing involves an attacker stealing an ML model and using it for malicious purposes.[71] This type of attack can compromise network security by allowing attackers to gain access to sensitive data and make unauthorized decisions.

---

[68] *See, e.g.*, Abdelfatteh Haidine *et al*, *Artificial Intelligence and Machine Learning in 5G and beyond: A Survey and Perspectives*, July 5, 2021, https://www.intechopen.com/chapters/77411; Jasneet Kaur *et al*, *Machine Learning Techniques for 5G and Beyond*, IEEE Access, Feb. 10, 2021, https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9321326.

[69] Zolotukhin, Mikhail et al, *On Assessing Vulnerabilities of the 5G Networks to Adversarial Examples*, IEEE Access, Dec. 1, 2022, https://ieeexplore.ieee.org/document/9968009.

[70] *See, e.g.*, Andrew Marshall et al, *Threat Modeling AI/ML Systems and Dependencies*, Microsoft, Nov. 2, 2022, https://learn.microsoft.com/en-us/security/engineering/threat-modeling-aiml; Lucian Constantin, *How data poisoning attacks corrupt machine learning models*, CSO Online, Apr. 12, 2021, https://www.csoonline.com/article/3613932/how-data-poisoning-attacks-corrupt-machine-learning-models.html.

[71] *See, e.g.*, Open Worldwide Application Security Project, ML05:2023 Model Stealing, https://owasp.org/www-project-machine-learning-security-top-10/2023/ML05_2023-Model_Stealing.html; Hailong Hu and Jun Pang, *Stealing Machine Learning Models: Attacks and Countermeasures for Generative Adversarial Networks*, Dec. 12, 2021, https://dl.acm.org/doi/10.1145/3485832.3485838.

- Adversarial Attack: Under this type of attack, the threat actor exploits the vulnerabilities of ML models by manipulating the input data to cause the ML model to make incorrect predictions or to compromise network security by causing the machine learning model to make incorrect decisions.
- Privacy Violation: ML algorithms require access to large datasets to learn patterns and make predictions. However, these datasets often contain sensitive information, such as personal information and network configurations. Privacy violations can occur if these datasets are accessed by unauthorized users, compromising the privacy of individuals and network security.[72]

6.2.2 Memory Unsafe Languages

Vendors using memory unsafe software coding languages within any hardware firmware, programmable read-only memory (PROM), hardware components, and accelerators, can provide threat actors an attack vector to execute specific attacks. As shown in Figure 5 blow, memory unsafe programming has existed for over 50 years since the first memory corruption found in 1972 by the Air Force to today.[73]

In November 2022, the NSA released a "Software Memory Safety" report to raise awareness of the risks associated with memory unsafe languages.[74] NSA shares that software languages such as C and C++ are examples of memory unsafe languages while C#, Go, Java, Ruby, and Swift are considered memory safe languages.

[72] *See, e.g.*, Katherine Jarmul, *Privacy Attacks on Machine Learning Models*, InfoQ, Aug. 6, 2019, https://www.infoq.com/articles/privacy-attacks-machine-learning-models/#:~:text=Privacy%20attacks%20against%20machine%20learning%20systems%2C%20such%20as,as%20predictive%20text%2C%20can%20expose%20highly%20sensitive%20information.

[73] United States Airforce, *Computer Security Technology Planning Study*, October 1972, https://csrc.nist.gov/csrc/media/publications/conference-paper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/early-cs-papers/ande72a.pdf.

[74] National Security Agency, *Software Memory Safety Report*, November 2022, https://media.defense.gov/2022/Nov/10/2003112742/-1/-1/0/CSI_SOFTWARE_MEMORY_SAFETY.PDF.

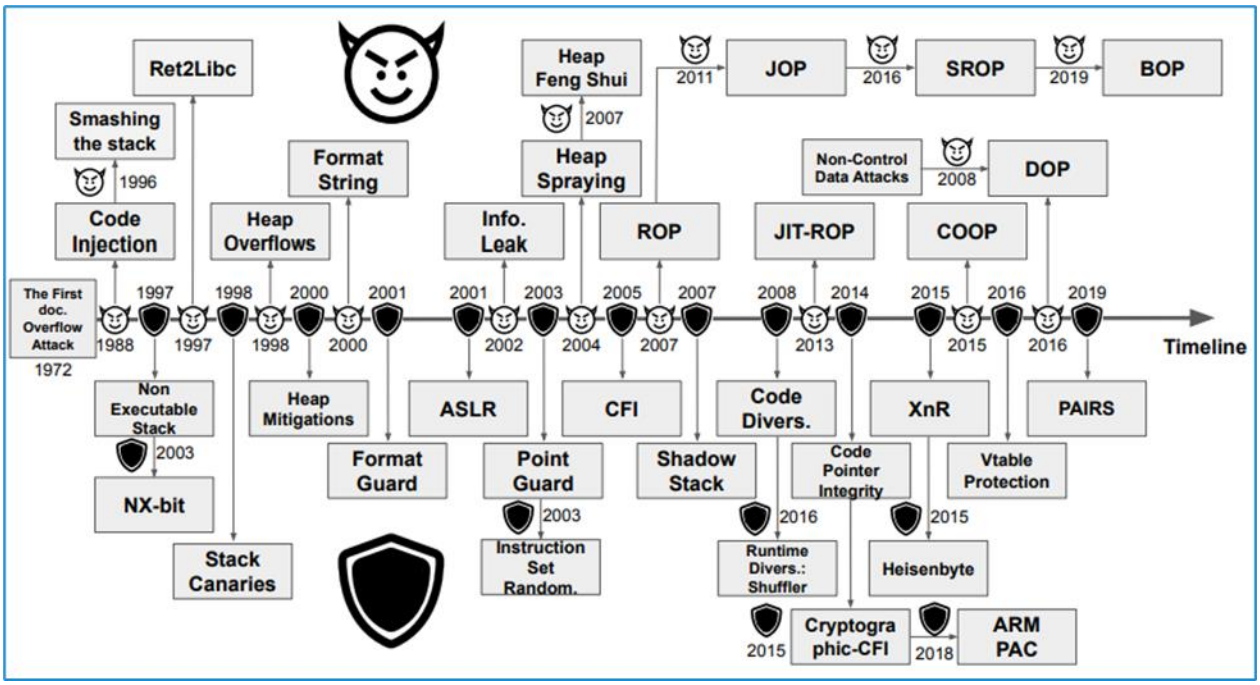

Figure 5 – Timeline for memory safety exploitation techniques[75]

Microsoft in 2019[76] and Google Chrome in 2021[77] both list memory unsafe programming languages causing 70 percent of all vulnerabilities requiring a security fix. These vulnerabilities are the result of Spatial, Temporal, and Type confusion errors.

6.2.2.1 Spatial Memory Errors

Spatial errors are more commonly known as 'out of bounds' memory read and write errors which allow a program to read and/or write past the limit of the object in memory.[78] If a list is created in a program with boundaries of one through ten, a memory unsafe language will allow the program to read or write the negative one or eleventh item on the list. Both of these events could allow the program to access a list of some other customer or user and allow a malicious actor to take advantage of a language that doesn't enforce memory boundaries.

---

[75] Mohamed Hassan, *Why is Memory Safety Still a Concern?*, Department of Computer Science, Columbia University, Apr. 9, 2020, https://www.cs.columbia.edu/~mtarek/files/candidacy_exam_syllabus.pdf.

[76] Microsoft, *Trends, challenges, and strategic shifts in the software vulnerability mitigation landscape*, 2019, https://github.com/Microsoft/MSRC-Security-Research/blob/master/presentations/2019_02_BlueHatIL/2019_01%20-%20BlueHatIL%20-%20Trends%2C%20challenge%2C%20and%20shifts%20in%20software%20vulnerability%20mitigation.pdf.

[77] Google, *An update on Memory Safety in Chrome*, 2021, https://security.googleblog.com/2021/09/an-update-on-memory-safety-in-chrome.html.

[78] *See* Alex Gaynor, Introduction to Memory Unsafety for VPs of Engineering, Aug. 12, 2019, https://alexgaynor.net/2019/aug/12/introduction-to-memory-unsafety-for-vps-of-engineering/.

6.2.2.2 Temporal Memory Errors

Temporal errors are classified as Use-After-Free (UAF), use of uninitialized memory, and wild and dangling pointer dereference.[79]

6.2.2.2.1 **Use-After-Free (UAF)**: UAF is a type of vulnerability that occurs when a program deletes or frees a portion of memory but does not clear the pointers to memory used in the program.[80] An example of this type of error would be if a list in a program was deleted and the memory is freed, later a new list is put in the same location of the freed list. The pointer to the memory is still there and can still reference the memory location.

6.2.2.2.2 **Uninitialized Memory**: This is the type of error caused in a section of code in a program that does not pre-initialize memory used for the data type defined in the code.[81] When a program is loaded into memory and that section of the code which is uninitialized is accessed, whatever value is leftover in physical memory will be accessible to the program currently occupying that portion of memory.

6.2.2.2.3 **Wild and Dangling Pointer Dereference**: Wild pointers and dangling pointers are types of memory pointers which do not point to a valid object of the appropriate type.[82] Wild pointers are pointers that have been used prior to a known initialized state. Dangling pointers are pointers which have not been freed or cleared in the code and allow the pointer to still exist.

6.2.2.3 Type Confusion

The program allocates or initializes a resource such as a pointer, object, or variable using one type, but it later accesses that resource using a type that is incompatible with the original type.[83] When the program accesses the resource using an incompatible type, this could trigger logical errors because the resource does not have expected properties.

6.2.3 Inadequate Zero Trust Implementations

Traditional management networks leverage a perimeter defense to keep threat actors out of the network which has created an implicit trust zone.[84] The existence of an implicit trust zone opens

---

[79] *See* USENIX, Presentation of Alex Gaynor, Quantifying Memory Unsafety and Reactions to It, 2019, https://www.usenix.org/sites/default/files/conference/protected-files/enigma2021_slides_gaynor.pdf.

[80] OWASP, Using Freed Memory, https://owasp.org/www-community/vulnerabilities/Using_freed_memory.

[81] *See, e.g.*, CQR, Uninitialized Memory Vulnerabilities, https://cqr.company/web-vulnerabilities/uninitialized-memory-vulnerabilities/.

[82] Dangling Pointer, Wikipedia, https://en.wikipedia.org/wiki/Dangling_pointer.

[83] Type Confusion, Hacking Portal, https://hackingportal.github.io/Type_Confusion/type_confusion.html.

[84] CTIA, Defining Zero Trust, Jan. 9, 2023, https://api.ctia.org/wp-content/uploads/2023/01/Defining-Zero-Trust-White-Paper-2023.pdf.

up the management network to insider attacks and easier lateral movement. Additionally, the network infrastructure consists of software-controlled hardware that has APIs that allow for remote control. As a result, most of the NMS platforms have relied upon this implicit trust domain to manage the network infrastructure and allow for automation and orchestration. Many network operators have taken steps to implement the principles of zero trust by leveraging single sign on, elimination of local accounts, reconfiguring their networks to use secure management protocols and APIs, utilization of network segmentation, and so forth. The network infrastructure vendors have enabled much of these capabilities but not all of the legacy hardware can support some of the latest advancements (e.g., SSH2, TLS 1.3). These challenges are cascaded upstream to the NMS platforms by layering in new ciphering algorithms at scale requires considerable compute resources in a large network.

The network operators, infrastructure vendors, and network management system vendors must work together to enable end-to-end adoption and implementation of zero trust principles. Ineffective zero trust implementations allow for a threat actor, whether internal or external, to compromise a platform and move laterally with more ease. Zero trust is an incremental process and will take years to effectively implement.[85] If or when a supply chain security vulnerability is compromised, an effective zero trust implementation should help limit the depth of the attack and allow the security operations teams to thwart the attack sooner in the kill chain.

6.2.4 Trusted Platform Module Vulnerabilities

Trusted Platform Module (TPM) is an international standard for a secure crypto processor that can function as a hardware root of trust using integrated cryptographic keys (see Section 5.1 on Hardware Root of Trust).

In late 2019, a team of academics from the Worcester Polytechnic Institute (USA), the University of Lübeck (Germany), and the University of California, San Diego (USA) disclosed two vulnerabilities known collectively as TPM-FAIL that could allow an attacker to retrieve cryptographic stored keys, impacting two widely used TPM solutions.[86]

The actual attacks on these two TPM technologies are commonly known as "timing leakage." In this type of attack, an external observer can record the time differences when the TPM is performing repetitive operations and infer the data being processed inside the secure chip -- all based on the amount of time the TPM takes to do the same thing over and over again. Researchers believe that this type of attack can be used to extract 256-bit private keys that are being stored inside the TPM.

Thanks to a concerted industry effort, both vulnerabilities have been fixed. However, this class of vulnerability presents an ongoing supply chain risk. Attacks such as these typically require some level of local control or probing to extract private keys from the TPM. Quite often, this is

---

[85] CISA, Zero Trust Maturity Model 2.0, April 2023, https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf.

[86] Press Release, Worcester Polytechnic Institute, WPI Researchers Discover Vulnerabilities affecting Billions of Computer Chips (Nov. 19, 2019), https://www.wpi.edu/news/wpi-researchers-discover-vulnerabilities-affecting-billions-computer-chips.

well suited to "intercept"-type attacks where components using a TPM are intercepted in the supply chain, compromised, then returned for later exploitation once installed in an operational system. To mitigate these types of attacks:

- Components using TPMs should be verified free from known side channel attacks.
- Secure distribution and storage practices should be used for all applicable components.

6.2.5 Continued Operation of End-of-Life Infrastructure for Service Providers

Communications providers face challenges in selecting best-of-breed components. Providers may not have the funds necessary to routinely perform the replacement of equipment. This can lead to vulnerabilities, particularly if a provider does not anticipate the decommissioning of end-of-life (EoL) devices. For example, a hardware manufacturer produced a small business line of routers that has reached end-of-life and warned of a vulnerability, tracked as CVE-2023-20025, that includes an authentication bypass issue residing in the management interface of the router.[87] A successful exploit could enable an attacker to gain root access to the device using a specially crafted HTTP request. Since the vulnerable devices are EoL, no security updates are expected for release.

Another example of a supply chain attack occurring as a result of EoL software took place in March 2023, with a subsequent attack in April 2023.[88] In this instance, X_Trader, an end-of-life financial stock trading software that was discontinued a couple of years ago and was no longer supported, was still available for download as of late 2022. The build/distribution server was compromised, and the attacker infected the software with malware. An individual downloaded the compromised software, onto the employee's personal computer.[89] The malware that the attacker had embedded into the X_Trader software was used to gain access to the employee's login credentials for the company. The attacker then used access granted by the malicious X_Trader software to infect the company's desktop application that was used to provide customers with a video conferencing and online communications platform. The attacker manipulated the application to add an installer that infected customers' networks. This attack represented what is believed to be the first documented instance of a supply chain attack (installing malware on the EoL software) that led to a second, subsequent supply chain attack (using the malware to gain access to a corporate application and infect that application through a separate installer). In April 2023, the same attack was found to have affected additional organizations, including those in the energy sector.

---

[87] *See* Pierluigi Paganini, *Critical bug in Cisco EoL Small Business Routers Will Receive No Patch*, Security Affairs Jan. 12, 2023, https://securityaffairs.com/140712/security/critical-bug-cisco-eol-routers.html; Cisco, *Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers Vulnerabilities*, Mar. 14, 2023, https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sbr042-multi-vuln-ej76Pke5.

[88] CISA, Supply Chain Attack Against 3CXDesktopApp, Mar. 30, 2023, https://www.cisa.gov/news-events/alerts/2023/03/30/supply-chain-attack-against-3cxdesktopapp.

[89] AJ Vicens, *3CX supply chain attack was the result of a previous supply chain attack, Mandiant says*, Cyberscoop, Apr. 20, 2023, https://cyberscoop.com/3cx-supply-chain-north-korea/.

6.2.6 Consumer Grade Infrastructure

A means for cost control that providers may employ is the use of non-enterprise-grade hardware. This can include consumer-grade networked devices such as routers, switches, storage, cameras, and other smart devices. An example of a vulnerability pertaining to a consumer-grade hardware device can be found with CVE-2022-43931 involving network router equipment manufactured by Synology. The vulnerability exists within the virtual private network (VPN) service on the device.[90] VPN services allow remote access to network resources behind the router. A successful exploit of the security flaw on a vulnerable device could allow arbitrary commands to be executed. The following list illustrates some of the differences and inherent security implications between enterprise and consumer hardware.[91]

1. Management – Consumer-grade hardware may lack automation, centralized updates, deployment mechanisms, and security capabilities required to efficiently protect from vulnerabilities.
2. Service – Enterprise-grade hardware may be bundled with vendor support, including on-site service and extended coverages to reduce downtime and ensure compatibility and performance.
3. Build quality – Consumer-grade hardware may use lower-quality parts and materials. Enterprise-grade hardware may be built for a longer life cycle.

6.2.7 Sourcing Telecommunications Infrastructure from Secondhand Markets

Decentralized second-hand markets for telecommunication equipment exist, with telecom providers, refurbishers, and brokers all fulfilling the role of buyer and seller.[92] In some instances, telecom operators may also source second-hand equipment from other operators. Second-hand equipment and second-hand markets as used in this report mean only used or discontinued equipment and are not intended to imply any connotation regarding the integrity of such equipment or marketplace. The term "grey market," for instance, is sometimes used to describe a market where a product is bought and sold outside the manufacturer's authorized trading channels or as the demarcation point between legal and illegal, where equipment can be purchased at lower cost and with little ability to trace the source.[93] While some organizations are implementing strategies to promote a circular economy, some providers may find themselves in situations where they rely on unofficial channels for procurement out of necessity.

---

[90] Sergiu Gatlan, *Synology Fixes Maximum Severity Vulnerability in VPN Routers*, Bleeping Computer, Jan. 3, 2023, https://www.bleepingcomputer.com/news/security/synology-fixes-maximum-severity-vulnerability-in-vpn-routers/.

[91] *See, e.g.*, Rutgers, Computer Standards: Reasons to Choose Enterprise Hardware, https://it.rutgers.edu/computer-standards/reasons-to-choose-enterprise-hardware.

[92] GSMA, *Strategy Paper for Circular Economy: Network Equipment*, March 2022, https://www.gsma.com/betterfuture/resources/strategy-paper-for-circular-economy-network-equipment.

[93] Arvato Systems, *Neither White nor Black, but Grey*, July 2021, https://www.arvato-systems.com/blog/grey-market-a-market-worth-billions.

Equipment supply chain delays, manufacturer mergers and dissolutions, and the need to obtain equipment quickly in certain circumstances can all result in telecom providers, both large and small, turning to the second-hand market to procure used hardware. Even with the best planning and financial resources directed at upgrading hardware, small providers are sometimes unable to source new hardware that is compatible with their size networks and thus must look to second-hand equipment. The need for used equipment is compounded by the predominance of single-source suppliers.

6.2.7.1 Security

Second-hand markets can include end of life equipment, which providers turn to when the equipment is the only source for replacing or adding a component that is compatible with legacy systems. As shown by some of the vulnerabilities identified in this report, used equipment, specifically end of life equipment, can pose a security risk for providers due to the inability to patch vulnerabilities or to verify the integrity of components that comprise the equipment and software. Used equipment may be subject to an increased risk of failure, thus impacting the availability of information services.[94] The standards of quality control can vary widely among refurbishers, and brokers may lack operational capacity to test, repair, or refurbish second-hand equipment. This can leave providers assuming greater risk associated with the reliability and security of used or refurbished equipment.

Manufacturers or suppliers have an interest in limiting operators from procuring secondary market equipment, and some of these reasons may align with provider concerns. For instance, cybersecurity risks may be created based on the flow of products through second-hand users, and manufacturers may not intend to offer continued patches for aging hardware.[95] Ultimately, manufacturers understand that this can cause brand damage, and inherently this potential for damage exists within the providers who operate using second-hand equipment.

The Commission also plays a role in guarding against certain secondary market equipment being used in providers' networks. In particular, the Commission's rules prohibit providers who receive government funds to remove and replace equipment identified on the Commission's list of equipment and services covered by Section 2 of The Secure Networks Act ("Covered List") from selling such equipment. The Commission's rules also specify the method providers must follow for disposing of equipment contained on the Covered List to further ensure such equipment is not used in telecommunications networks.[96]

6.2.7.2 Response

Addressing supply chain issues to increase the amount of up-to-date equipment available to both large and small providers would decrease the need for used equipment while also better

---

[94] Brien Posey, *Is It Ever OK To Use Refurbished Servers?*, Redmond Magazine, Mar. 2, 2023, https://redmondmag.com/articles/2023/03/02/is-it-ever-ok-to-use-refurbished-servers.aspx.

[95] GSMA, *Strategy Paper for Circular Economy: Network Equipment*, March 2022, https://www.gsma.com/betterfuture/resources/strategy-paper-for-circular-economy-network-equipment.

[96] *See Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, WC Docket No. 18-89, Second Report and Order, FCC 20-176 (2020).

positioning providers' supply chain security. Used equipment, where required, can also be sourced from trusted suppliers. Manufacturers may choose to offer a refurbishing program that incorporates testing, upgrades to the latest software versions, quality assurance, and secure delivery in original packaging. These programs can have strict procedures for handling, storing, and transporting equipment, upholding security requirements within the supply chain.[97]

Furthermore, as recommended in the CSRIC VIII Open RAN Report, "Organizations should define and adopt a process for managing software and the security risk of third-party components that fits into an organization's existing SDLC to ensure supply chain integrity. Putting security at the core of the SDLC enhances Open RAN system security."[98] In the context used within the ORAN Report, SDLC is referred to as part of the Software Development Life Cycle rather than the more encompassing Systems Development Lifecycle, which is also commonly referred to as SDLC. In particular, Section 5.2.1 of the ORAN Report mentions "components" which, depending on the context, could mean software or hardware components.

7 Summary of Key Findings

In today's highly disaggregated supply chain model, supply chain security is presented with challenges that are not easy to solve. In many of today's compute platforms, the hardware and software components are sourced from global suppliers and open source communities. It is encouraging to see the governmental agencies and several industry bodies working independently to address this broad attack vector.

In general, supply chain attacks can be addressed by considering:

- Prevention and detection of vulnerability insertions in the supply chain itself, and
- Operational cybersecurity capabilities specifically designed to mitigate the exploitation of inserted vulnerabilities.

Although the focus of this report is on securing the supply chain, specific operational capabilities are noted in this report when they also serve to minimize the impact of supply chain vulnerabilities.

For example, the publication Defending Against Software Supply Chain Attacks,[99] released by CISA and NIST, recommends actions to mitigate malicious or vulnerable software that may be inserted via the supply chain. This publication specifically noted security architectural techniques in support of this goal:

> "Using deliberate network segmentation, organizations can mitigate the effects of

[97] Ericsson, *Can the telecom industry materialize a sustainable future with Product Reuse?*, September 2022, https://www.ericsson.com/en/blog/2022/9/product-reuse-services-for-telecom-networks-equipment.

[98] FCC, CSRIC VIII, *Report on Challenges to the Development of ORAN Technology and Recommendations on How to Overcome Them*, December 2022, at p. 39, https://www.fcc.gov/file/24520/download (ORAN Report).

[99] CISA, Defending Against Software Supply Chain Attacks, https://www.cisa.gov/sites/default/files/publications/defending_against_software_supply_chain_attacks_508_1.pdf.

> software vulnerabilities and associated exploits, as well as aid incident response and recovery. Segmentation helps confine a vulnerability or attack to portion of a customer's enterprise. Organizations can also achieve such mitigation by implementing endpoint-based micro-segmentation with host-based firewalls or agents. Micro-segmentation can be part of a 'zero trust' architecture or implemented on its own."[100]

As we emphasize in this report, hardware relies on software so it can function as designed. Likewise, NMS is a collection of software as defined in Section 3.2 and thus recommendations will necessarily center around software. This section will highlight some of the key findings that CSRIC VIII has collected post the analysis of the sections above.

The vulnerabilities and threats facing small providers are much the same as for large providers – some attacks target the equipment most commonly used by these providers while supply chain attacks are typically indiscriminate in the size or type of entity they affect. What is different for small providers is the resources they have available to devote to guarding against or recovering from supply chain attacks. The Commission and federal departments and agencies can help strengthen small providers' supply chain security by offering free cyber resources such as CISA's vulnerability scanning[101] and funding to hire and train cyber professionals, especially in less populated areas.

7.1 Supply Chain Security Specifications and Tools

ATIS, TIA, and MITRE have taken broad steps through the development of their supply chain security specifications, recommendations, and tools that can assist a CSP when comparing multiple vendors. These specifications, though different, can provide foundational security controls and requirements that a CSP can require of a vendor that is providing infrastructure and/or network management systems solutions.

Currently, IETF is developing a framework of related specifications in their Supply Chain Integrity, Transparency, and Trust (SCITT) Work Group.[102] The group is looking to address many of the security concerns at the low level through the development of new specifications for software and hardware products.

7.2 Government Activities

The U.S. government has pushed this topic to the forefront for the industry. Their support of public/private partnerships and information sharing will bear fruit for years to come. Their leadership can help erase or ease some of the challenges when vendors are developing, manufacturing, and/or sourcing software and hardware components from various countries. In September 2022, the Office of Management and Budget published a memorandum to all agency

---

[100] *Id*. at 10.

[101] CISA, Vulnerability Scanning, https://www.cisa.gov/resources-tools/services/cisa-vulnerability-scanning.

[102] IETF, Supply Chain Integrity, Transparency, and Trust (SCITT) Work Group, https://datatracker.ietf.org/group/scitt/about/.

heads directing them to require SBOMs for all new software purchases where the software is defined as critical.[103] By requiring an SBOM delivery during the procurement engagement, this will encourage the development, production, and delivery of an SBOM with a product or service. The ability to develop the required processes and procedures to allow an agency to mandate and authenticate the provenance of software and/or individual software components is an important step. Looking beyond just software and identifying that a hardware bill of materials (HBOMs) is just as critical since hardware comes with additional software that may not be captured in the SBOM. This would require voluntary participation from the various countries to ensure that the quality and accuracy of the information sharing is trusted and reliable. This information sharing is more critical for open source software vendors and/or developers who may have ties with unfriendly countries and/or known threat actors.

7.3 Zero Trust Principles

Many of the sources identified above, encourage the adoption of zero trust principles in not only the supply chain but also in the operational networks. One of the key principles associated with zero trust is to limit the blast radius when an operational technology is compromised. Likewise, the premise of zero trust is that the network is already compromised. The underlying message in the various reports above is that no one can stop supply chain attacks so therefore implement the hardware and software using a zero trust architecture. For example, network segmentation is one zero trust principle that is referenced repeatedly.

7.4 HBOMs and SBOMs

CSRIC VIII discussed SBOMs extensively in its September 2022 report.[104] SBOMs continue to be an area of opportunity for the industry to mature both from the publication of machine readable SBOMs and the vulnerability scanning tools against these SBOMs. Likewise, the industry should consider HBOM in concert with SBOM since essentially all hardware consists of software that needs to be accounted for in the SBOM. There is a significant gap in the standardization of HBOMs unlike SBOMs which have two primary leading formats - SPDX and Cyclone DX. HBOMs should include configuration, provenance of the component(s), and obsolescence of any component(s). Each individual component should have a unique SBOM, or the component's software should be reported in a higher level platform SBOM.

7.5 Memory Unsafe Languages

Since NSA's publication in late 2022 of its Software Memory Safety report, the U.S. government, has pursued a conversation on this issue with the cybersecurity industry. The challenges with the migration from unsafe to safe languages is that some of the telecommunications related code bases have been around for decades. The code bases have

---

[103] Memorandum (M-22-18) for the Heads of Executive Departments and Agencies, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices, September 14, 2022, https://www.whitehouse.gov/wp-content/uploads/2022/09/M-22-18.pdf

[104] CSRIC VIII Software Supply Chain Report at 14-15, 22-23.

evolved themselves over the years to support new protocols, standards based specifications, and proprietary functions. Nevertheless, it will take years for vendors to effectively migrate from unsafe languages due to the complexities of the generational specifications identified by the various SDOs.

7.6 ML/AI

ML and AI will have generational impacts on CSPs. Currently, use of ML/AI is in the early stage of deployment, and enterprises in general are devoting more resources to understanding its potential uses in production environments. In addition, the advent of quantum computing will enable more robust ML/AI capabilities. Therefore, the time is now to begin deeper conversations on security best practices, specifications, recommendations, and guidelines for ML and AI in the global CSP ecosystem.

7.7 Platform Security

Securing the system from supply chain attacks can be facilitated through strong platform security measures. The main building blocks for platform security can be listed as Root of Trust, Secure Storage, Secure Boot, and Secure Debug. A flexible and robust platform security solution also requires a solid and futureproof key management service utilizing up to date hardware crypto engines and TRNG engine.

A Hardware Root of Trust must be inherently trusted; therefore, it must be secure-by-design providing a foundation on which all secure operations of a computing system depend. Secure Storage is a service in hardware to store data objects securely in a non-volatile fashion on the board. The processing on the product must be brought up in a secure state. Secure Boot is the basic feature that provides this security and trustworthiness. Secure Debug is one of the most important platform security requirements, as access to debug ports should be locked to maintain operational security and a secure unlock should be supported when access is required by an authorized entity.

Hardware vulnerabilities may also lurk in legacy platforms or discontinued products still in use thus representing a persistent risk across infrastructure and NMS supply chains. End users should maintain awareness of all products used to maintain and operate their critical infrastructure networks. In particular, CSPs must maintain vigilance over firmware updates that may not address key elements, including SDKs or specific SOC components. Of particular note, the CISA co-authored paper "Shifting the Balance of Cybersecurity Risk," cites the European Union's Cyber Resilience Act, which reflects the European Commissions' perspective of manufacturers' responsibilities to prevent introducing vulnerable products into the marketplace. The Commission may wish to consider a working group to assess the value of these governmental policy developments in a future CSRIC Charter.

7.8 Network Management

Network Management Systems encompass a broad range of functionality realized in software and deployed into various infrastructure environments, dictated by network operator needs. The

software used in NMS, like other modern software systems, typically includes a mix of proprietary, third party and Open Source Software.

The primary role of an NMS is for the roll out, configuration management, node/service monitoring, device management, and software management across all network nodes-such as core, transport, and radio access nodes. In the case of radio access nodes, an NMS may be responsible for the management of 10s, 100s, 1000s or even 10,000 nodes, depending on the network size. It is therefore critical that NMS solutions support robust user access controls and that network operators incorporate such controls their networks. Typical access controls should consist of user authentication and authorization, based on granular user roles and policies, with a least privilege mindset, plus capabilities that enable tracing of user activities.

NMS interfaces to network nodes, via so called southbound interfaces, should be secured to ensure only authenticated and authorized access is allowed and depending on the sensitivity of the information traversing such interfaces, enforce ciphering and integrity protection.

Depending on an operator's deployment architecture, an NMS may also communicate with other systems, such as an umbrella network management system or a service orchestration system, via so called northbound interfaces. Such interfaces should also enforce authentication and authorization and ciphering and/or integrity protection depending on the sensitivity of the information being exchanged. NMS access to the internet is not allowed, however secure access (e.g., VPN) is provided to NMS vendors to enable support services.

NMS should support and use security controls which can detect if received software artifacts, such as software builds and configuration files for the NMS platform and the managed and monitored nodes, have been tampered with and provide secure storage of such artifacts.

NMS, like any other software system, should have robust secure software development and software supply chain security controls in place that are adhered to and continuously re-evaluated for the complete lifecycle of the NMS.

8 Summary of Key Recommendations

The table in this section summarizes specific vulnerabilities and the associated recommended mitigations discussed in this report. This table is neither exhaustive nor complete but highlights important areas focus in protecting the supply chain.

To that end, we note that many other security and supply chain practices should be implemented (as noted in the various supply chain standards and best practices referenced in this report). For example, all of the noted supply chain functions referenced in Section 3.4.1 should be subject to best-in-class cybersecurity practices to mitigate the insertion of vulnerabilities that can be leveraged in a supply chain attack.

We also note that this report focuses on software controlled hardware aspects and should be read in the context of CSRIC VIII's first report on "Recommended Best Practices to Improve

Communications Supply Chain Security,"[105] which provides numerous mitigating recommendations the software supply chain.

Vulnerabilities	Recommended Mitigation
Unpatched User Equipment (UE) and Devices (e.g., IoT) and Network Infrastructure Devices	▪ Patch vulnerable devices whenever possible to reduce exposure risks across the organization. ▪ Use device discovery and classification to identify devices with vulnerable components by enabling vulnerability assessments, which identifies unpatched devices in organizational networks; set workflows for initiating appropriate patch processes. ▪ Ensure robust device update and patching capabilities; never require physical access to a device for recovery (unless there is physical damage to the device).
Operating Legacy Applications (e.g., Web Server Components)	▪ Extend vulnerability and threat detection beyond the firewall to identify Internet-exposed infrastructure running legacy applications. ▪ Adopt comprehensive operational technology solution(s) to monitor devices (e.g., UE, network infrastructure), respond to threats, and increase visibility in order to detect and alert when devices with legacy software, such as Boa, are used as an entry point to a network.
Superfluous Internet Connectivity	▪ Reduce the attack surface by eliminating unnecessary Internet connections to the UE devices, network infrastructure, and network management systems in the network. If a device is compromised in the supply chain then it could attempt to communicate with Internet based command and control servers that are controlled by the threat actor. ▪
Lack of Network Segmentation	▪ Apply network segmentation to prevent an attacker from moving laterally and compromising other network assets after intrusion. For example, IoT devices and network management platforms should be isolated with firewalls.
Lax Intrusion Detection Rules	▪ Implement effective intrusion detection and prevention solutions to protect critical network infrastructure and network management systems.

[105] FCC, CSRIC VIII Report on Recommended Best Practices to Improve Communications Supply Chain Security, September 2022, https://www.fcc.gov/file/23839/download.

Vulnerabilities	Recommended Mitigation
	▪ Configure thorough detection rules to identify malicious activities.
Poor Access Security	▪ Apply more stringent access controls to critical management networks and network services including multi-factor authentication. ▪ Apply the principle of least privileged access. ▪ Monitor network and UE device logs for anomalous or suspicious activity. ▪ Provide the ability to audit system configuration changes and flag anomalous activities. ▪ Set a baseline for normal network traffic and monitor for aberrations. ▪ Implement improved security monitoring at ingress and egress points of the CSP's network and at any network interconnection boundary.
Poor Response and Recovery Plans	▪ Review and ensure the effectiveness of incident response and recovery plans.
Non-Existent/Weak ML/AI Data Poisoning Protections	▪ Implement a ML/AI data validation process that checks for malicious data before it is included in the training dataset. ▪ Implement anomaly detection algorithms to identify and flag suspicious data points.
Non-Existent/Weak ML/AI Theft Protections	▪ Implement robust security protocols, such as encryption and access controls, to protect machine learning models. ▪ Implementing detection mechanisms that can identify when a model has been stolen to help prevent attackers from using the model for malicious purposes.
Lack of ML/AI Adversarial Inputs Protections	▪ Implement robust machine learning models that are resistant to adversarial attacks. ▪ Implement detection mechanisms that can identify when an adversarial attack is occurring.
Weak/Insufficient Data Privacy Protections	▪ Implement access controls and encryption protocols to protect sensitive data. ▪ Implement mechanisms that allow individuals to control access to their personal data to prevent unauthorized access to sensitive information.

Vulnerabilities	Recommended Mitigation
Compromised Hardware Integrity	▪ Require Infrastructure and NMS vendors to provide HBOM(s) with corresponding SBOMs for each individual component. ▪ Implement various hardware platform security mechanisms including use of HRoT to ensure platform integrity. ▪ Utilize security capabilities provided by the platform security to mitigate risk of HW manipulation.
Memory Unsafe Languages	▪ Migrate from programming languages which provide little or no inherent memory protection to memory safe languages. Wholesale migration may not be an option for some groups so incremental change to the most exposed code, code with the highest privilege, or code with the highest bug count could be considered first.[106] ▪ Implement static and dynamic application security testing (SAST/DAST) tools to reduce memory un-safe vulnerabilities. ▪ Increase awareness and advocacy. Learn lessons from MANRS (Mutually Agreed Norms for Routing Security) to create a set of practices to improve memory safe programming.
Unprotected Data at Rest	Use a Storage Root Key to protect vendor and user sensitive data and key material stored locally on device
Compromised HRoT	Protect integrity of HROT (e.g., hash of Public Root Keys) by using hardware based Secure Storage (e.g., One-time programmable (OTP) electrical fuses, PUF)
Compromised Device External Interfaces	▪ Implement authentication and access controls on all external interfaces, in particular test and debug ports. ▪ Allow only expected functions/operations and reject all other access attempts. ▪ Close all test and debug ports which are not supposed to be open in the field/production networks
Compromised Device Internal Interfaces	Implement authentication and access controls on all internal interfaces, in particular test - and debug ports
Weak Ciphers and	Utilize hardware crypto accelerators and a TRNG

[106] National Security Agency, Software Memory Safety, November 2022, https://media.defense.gov/2022/Nov/10/2003112742/-1/-1/0/CSI_SOFTWARE_MEMORY_SAFETY.PDF.

Vulnerabilities	Recommended Mitigation
Entropies	
Key Leakage/Compromise	Protect key material by hardware-rooted device unique Storage Root Key

Table 5 – Summary of Key Vulnerabilities and Recommended Mitigations

9 Additional Recommendations for the Commission

Both small and large providers are challenged with infrastructure and network management systems supply chain security. As noted in this report, this is a complicated security domain and should be broken out into specific focus areas. These are additional areas where the Commission could engage with other entities, as appropriate, such as government agencies and industry, to explore these issues. Recommendations include:

- An examination of the use of ML and AI in a CSP environment. ML and AI based software including network management systems are on the rise. AI uses ML algorithms to create datasets that the AI engine can use to make decisions. Many of the communication vendors are embedding ML/AI capabilities in the products and/or services being delivered. The old expression, "Garbage In, Garbage Out",[107] is instructive here - if the dataset is corrupted then the AI engine will make decisions based on poisoned data.[108] For example, if an ML algorithm is modified in the delivered network management system software so that it poisons only 0.01% of prominent deep-learning datasets then it is sufficient to poison the entire dataset.[109] Protecting the integrity of the data sets is paramount to the effective operation of these technologies in a CSP network.

  AI engines, such as ChatGPT,[110] have evolved significantly and the adoption of this technology for all kinds of enterprise applications is expanding rapidly. There has not been a comprehensive security study related to the use of this technology in a CSP environment. A key question is whether there are any potential national security risks associated with the use of ML/AI in a domestic CSP's network. Securing our software supply chain is critical as discussed in this report. Compromised software code can result in catastrophic disruptions to a CSP and the services that are delivered. In April 2023, it was reported that Samsung

[107] Garbage In, Garbage Out, Wikipedia, https://en.wikipedia.org/wiki/Garbage_in,_garbage_out.

[108] Danny Palmer, *The Next Big threat to AI might already be Lurking on the Web*, ZDNET, Mar. 2, 2023, https://www.zdnet.com/article/the-next-big-threat-to-ai-might-already-be-lurking-on-the-web/.

[109] *Id.*

[110] OpenAI, ChatGPT, https://openai.com/.

employees accidentally leaked source code by uploading it to ChatGPT.[111] Additionally, ChatGPT was shut down in March 2023 due to some code bugs that allowed wrong users to see other user's data including the exposure of ChatGPT Plus members.[112]

As this technology continues to mature and be seen as an unreplaceable asset to help CSPs operate more efficiently, a thorough security study needs to be completed so that the U.S. based CSPs, software and hardware vendors, and cloud service providers can take appropriate steps to secure the technology in the supply chain.

- Study the security impacts of memory unsafe languages in a CSP network. Additionally, the study should explore the challenges with migrating to memory safe languages and suggest some practical recommendations for the incremental transition to memory safe languages. The study could provide a listing of the appropriate industry bodies for the FCC to participate in the standards, specifications, and preparation of best practices.

- Assist with the standardization of HBOM formats and uses. Relating to infrastructure, HBOMs provide a critical view into the ingredients of the procured and/or operating hardware that includes all motherboards, graphics cards, interfaces, expansion modules, and baseband modems. Additionally, individual HBOMs should be provided for each individual component so that the CSP has full transparency into the delivered products. The HBOM should provide visibility and traceability of the hardware components, firmware, and the systems.[113]

  Additionally, an HBOM should be considered in concert with an SBOM so that the two are better understood in the supply chain. Understandably, as the product and/or service traverses the supply chain, modifications to the hardware and software builds may take place, and these modifications should be captured accurately, securely, and provenance should always be trusted and verifiable.

- To assist CSPs with identifying anomalous behaviors, facilitate a study to investigate the benefits and feasibility of standardizing 3GPP network function (NF) event logging, for instance event definitions, uniform identifiers, triggers, and determine the scope and which standards body would be most suited to such an undertaking.[114] For example, a misbehaving network function and/or UE would generate a known set of events (e.g., UE Initiated Attach, UE Initiated Detach, NRF Token Request), and each event should generate a series of

---

[111] Shweta Sharma, *Samsung Bans Staff AI Use Over Data Leak Concerns*, CSO, May 2, 2023, https://www.csoonline.com/article/3695170/samsung-bans-staff-ai-use-over-data-leak-concerns.html.

[112] OpenAI, *March 20 ChatGPT Outage: Here's What Happened*, Mar. 24, 2023, https://openai.com/blog/march-20-chatgpt-outage.

[113] Intel, Transparent Supply Chain, https://www.intel.com/content/www/us/en/products/docs/servers/transparent-supply-chain.html.

[114] Press Release, CISA, CISA Announces Plans to Establish Logging Made Easy Service (Apr. 20, 2023), https://www.cisa.gov/news-events/news/cisa-announces-plans-establish-logging-made-easy-service.

individual log events on various NFs (e.g., gNB, AMF, AUSF, NRF, SMF, UPF). By leveraging uniform identifiers for these events, a CSP would be better positioned to identify a security event (e.g., UE sourced DDoS attack, malicious NF) in a multivendor 5GS since all vendors would be using uniform IDs for the various 3GPP events. This would mirror what the industry has done with Linux through the standardization of common uniform system event ID definitions, which is the underlying capability that allows for various system level security attack detections possible via the MITRE ATT&CK framework.[115] MITRE has evolved their ATT&CK framework for a 5G environment and now has created a 5G Hierarchy of Threats, also known as FiGHT.[116] In the way the ATT&CK framework leverages the Linux audit daemon (auditd), which is the system level event ID numbering/cataloging framework, the FiGHT framework will also leverage auditd's common system level event IDs, but it will also need common NF level event IDs, which do not exist today. If any 5GS infrastructure (e.g., UE, RAN, Core) or NMS' hardware and/or software is compromised in the supply chain, this capability could potentially shorten the time of security event detection by standardizing the indicators of compromise across all vendors.

- Explore the benefits and practicality of a runtime security capability within a 5GS that could potentially allow for faster detection of anomalous behaviors/activities at the 3GPP NF (application) level (e.g., gNB, AMF, SMF, UPF, AUSF, NRF, NEF). Hardware and software vendors have the most knowledge on the integrals of the solutions they are productizing and delivering to the CSPs. By way of example, automotive manufacturers have the most knowledge on their products and they have developed robust runtime event monitoring capabilities in vehicles that will generate engine error codes when a module, sensor, or other component starts experiences degradation or malfunction. This runtime security event detection capability could be developed for the communications industry to help CSPs identify security anomalies within the network functions. This capability could potentially shorten the time of security event detection possibly to near real-time.

[115] MITRE, ATT&CK Framework, https://attack.mitre.org/.

[116] MITRE, FiGHT Framework, https://fight.mitre.org/.

Appendix A – Resources for Small Providers

In its September 2022 report, CSRIC VIII recommended that resources tailored to the needs and capabilities of small communications providers would help those providers as they work to secure their networks. Following up on that recommendation, CSRIC VIII has identified complementary resources to assist small communications providers with securing their supply chain. While these resources do not specifically mention infrastructure and network management systems, they do provide concrete supply chain guidance for small communications providers. The resources also benefit from being created by small and mid-sized communications and information technology providers based on the needs and capabilities of those providers identified.

- **Securing Small and Medium-Sized Business Supply Chains**[117] – CISA in collaboration with the Communications Sector Coordinating Council and the Information Technology Sector Coordinating Council provides a resource handbook to reduce information and communications risks. This handbook includes six use cases to help SMBs recognize common ICT supply chain risk challenges and provides practical and actionable measures they can take to mitigate these risks. The use cases are based on fictional ICT companies and present scenarios that these SMBs may face. They also highlight one or more of the six risk categories, propose potential options that the fictional company may consider, provide a short summary of costs and benefits associated with implementing the proposed options, and provide a section of government and industry mitigation resources that can be accessed for more detail.
- **Operationalizing the Vendor SCRM Template for Small and Medium-Sized Businesses**[118] - This guide assists small and medium-sized businesses in mitigating ICT supply chain risk with a specific focus on making the enterprise Vendor Template more accessible and usable for SMBs.
- **Cyberplanner**[119] – The FCC provides an online resource to help small businesses create customized cybersecurity plans by creating and saving a custom cyber security plan that includes network and operational security, choosing from a menu of expert advice to address specific business needs and concerns.
- **Communications Supply Chain Risk Information Partnership**[120] - The Communications Supply Chain Risk Information Partnership (C-SCRIP) program is

---

[117] CISA, Securing Small and Medium-Sized Business Supply Chains, Jan. 26, 2023, https://www.cisa.gov/sites/default/files/publications/Securing-SMB-Supply-Chains_Resource-Handbook_508.pdf

[118] CISA, Operationalizing the Vendor Supply Chain Risk Management Template for Small and Medium-Sized Businesses, https://www.cisa.gov/sites/default/files/publications/ict-scrm-task-force_smb-operationalizing-vendor-template_508.pdf. A spreadsheet version available for download at https://www.cisa.gov/resources-tools/resources/ict-scrm-task-force-vendor-template.

[119] FCC, Cyberplanner, https://www.fcc.gov/cyberplanner.

[120] NTIA, Communications Supply Chain Risk Information Partnership, https://cscrip.ntia.gov/.

designed to share supply chain security risk information with trusted communications providers and suppliers. The program seeks to improve small and rural communications providers' and equipment suppliers' access to information about risks to key elements in their supply chain. NTIA tailors risk information to be relevant and accessible to the C-SCRIP community. Additionally, C-SCRIP shares public security alerts, information on grant funding opportunities from government partners, and conducts relevant training events.

Appendix B – Glossary[121]

Term	Description
Bare Metal Server	A physical computer server that is used by one consumer, or tenant, only. Each server offered for rental is a distinct physical piece of hardware that is a functional server on its own. They are not virtual servers running in multiple pieces of shared hardware. In terms of virtualization, a bare metal server makes resources more readily available to one "tenant", network latency is minimized for better performance, and the tenant enjoys root access. Bare metal is highly customizable, and the tenant may optimize the server based upon their individual needs.
Best Practice	A method or technique that users generally accept as superior because it produces results that are superior to those achieved by other methods or techniques.
Cloud Computing	The on-demand availability of computer system resources, especially data storage (cloud storage) and computing power, without direct active management by the user. Large clouds often have functions distributed over multiple locations, each location being a data center. Cloud computing relies on sharing of resources to achieve coherence and typically using a "pay-as-you-go" model which can help in reducing capital expenses but may also lead to unexpected operating expenses for unaware users.
DAST	Dynamic Application Security Testing – a non-functional testing process where one can assess an application using certain techniques and the end result of such testing process covers security weaknesses and vulnerabilities present in an application. This testing process can be carried out either in manual way or by using automated tools.
DevSecOps	Development, Security, and Operations – the integration of security at every phase of the software development lifecycle, from initial design through integration, testing, deployment, and software delivery.[122]

[121] Unless otherwise noted, term descriptions are sourced from Wikipedia.

[122] IBM, DevSecOps, https://www.ibm.com/cloud/learn/devsecops.

Term	Description
HBOM	Hardware bill of materials lists every physical component used to build a product and/or make up a platform.
HROT	Hardware Root of Trust - The foundation on which all secure operations of a computing system depend. It contains the keys used for cryptographic functions and enables a secure boot process. It is inherently trusted, and therefore must be secure by design. The most secure implementation of a root of trust is in hardware making it immune from malware attacks. As such, it can be a stand-alone security module or implemented as security module within a processor or system on chip (SoC).[123]
Hyperscale computing	The ability of a computer architecture to scale appropriately as increased demand is added to the system. This typically involves the ability to seamlessly provide and add compute, memory, networking, and storage resources to a given node or set of nodes that make up a larger computing, distributed computing, or grid computing environment. Hyperscale is necessary to build a robust and scalable distributed system.
MSP	Managed Service Provider – a third-party company that remotely manages a customer's information technology (IT) infrastructure and end-user systems. Small and medium-sized businesses (SMBs), nonprofits and government agencies hire MSPs to perform a defined set of day-to-day management services. These services may include network and infrastructure management, security, and monitoring.[124]
NMS	Network Management System – the set of applications that enable a CSP to intelligently manage and operate a network, network segments, and associated network services, including the individual devices that are delivering the communications services.
OSS	Open Source Software – software that can be accessed, used, modified, and shared by anyone and usually distributed under licenses that comply with the definition of "Open Source" provided

[123] Rambus, Hardware Root of Trust: Everything You Need to Know, Oct. 29, 2021, https://www.rambus.com/blogs/hardware-root-of-trust/.

[124] Alexander S. Gillis, *Definition: Managed Service Provider (MSP)*, TechTarget, https://www.techtarget.com/searchitchannel/definition/managed-service-provider.

Term	Description
	by the Open Source Initiative.
Proprietary Software	Computer software for which the software's publisher or another person reserves some licensing rights to use, modify, share modifications, or share the software, restricting user freedom with the software they lease. It is the opposite of open source or free software. Non-free software sometimes includes patent rights.
RCE	Remote Code Execution – the process by which an agent can exploit a network vulnerability to run arbitrary code on a targeted machine or system. For example, in an RCE attack, hackers exploit a remote code execution vulnerability to run malware. RCE can prompt the targeted device to perform code execution, running their own programming in its place, and thus enabling the hacker to gain full access, steal data, carry out a full distributed denial of service (DDoS) attack, destroy files and infrastructure, or engage in illegal activity.[125]
SAST	Static Application Security Testing – a method to secure software by reviewing the source code of the software to identify sources of vulnerabilities.
SBOM	Software Bill of Materials – a list of all open source and third-party components present in a codebase. An SBOM may lists the licenses that govern those components, the versions of the components used in the codebase, and their patch status, which allows security teams to quickly identify any associated security or license risks.[126]
SDLC	Software Development Lifecycle – the complete process of developing a software solution with different stages and steps to bring the software from ideation to building, deployment, and maintenance.[127]
Secure-by-Default	The principle that IT products to be resilient "out of the box" to prevent exploitation techniques without additional charge or

[125] N-able, Remote Code Execution Overview, Aug. 29, 2019, https://www.n-able.com/blog/remote-code-execution.

[126] Fred Bals, *What is a Software Bill of Materials*, Synopsis, Mar. 16, 2022, https://www.synopsys.com/blogs/software-security/ software-bill-of-materials-bom/.

[127] Amrita Pathak, *Software Development Life Cycle (SDLC): A Complete Guide*, Geekflare, July 1, 2022, https://geekflare.com/software-development-life-cycle-sdlc-guide/.

Term	Description
	additional steps, and to make customers aware that deviation from safe defaults increases the likelihood of compromise.
Secure-by-Design	The principle of building technology products that can reasonably be expected to protect against malicious cyber actors gaining access to devices, data, and connected infrastructure.
Small Provider	For purposes of this report, small providers are defined as those with 250,000 or fewer broadband subscribers. This definition is consistent with prior Commission action to adopt tailored approaches for small entities.[128]
SSDF	Secure Software Development Framework – NIST's set of fundamental, sound, and secure software development practices based on established secure software development practice documents from organizations such as BSA, OWASP, and SAFECode.
Virtualization	Emulation of a physical computer system.
Zero Trust	A security model, also known as zero trust architecture (ZNA), zero trust network architecture or zero trust network access (ZTNA), and sometimes known as perimeterless security, describes an approach to the design and implementation of IT systems. The main concept behind the zero trust security model is "never trust, always verify," which means that devices should not be trusted by default, even if they are connected to a permissioned network such as a corporate LAN and even if they were previously verified.

[128] *See* Small Business Exemption from Open Internet Enhanced Transparency Requirements, GN Docket No. 14-28, Order, FCC 17-17 (rel. Mar. 2, 2017).