ATIS 5G Supply Chain Standard

Creating the Foundation for Assured 5G Networks

ATIS-I-0000087
September 2021

atis

COPYRIGHT INFORMATION

ATIS-I-0000087

Alliance for Telecommunications Industry Solutions

1200 G Street, NW, Suite 500

Washington, DC 20005

NOTICE OF DISCLAIMER AND LIMITATION OF LIABILITY

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER, NO REPRESENTATION OR WARRANTY IS MADE OFMERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES THAT ANY AND ALL USE OF OR RELIANCE UPON THE INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

NOTE - The user's attention is called to the possibility that compliance with this document may require use of an invention covered by patent rights. By publication of this document, no position is taken with respect to whether use of an invention covered by patent rights will be required, and if any such use is required no position is taken regarding the validity of this claim or any patent rights in connection therewith. Please refer to [http://www.atis.org/legal/patentinfo.asp] to determine if any statement has been filed by a patent holder indicating a willingness to grant a license either without compensation or on reasonable and non-discriminatory terms and conditions to applicants desiring to obtain a license.

TABLE OF CONTENTS

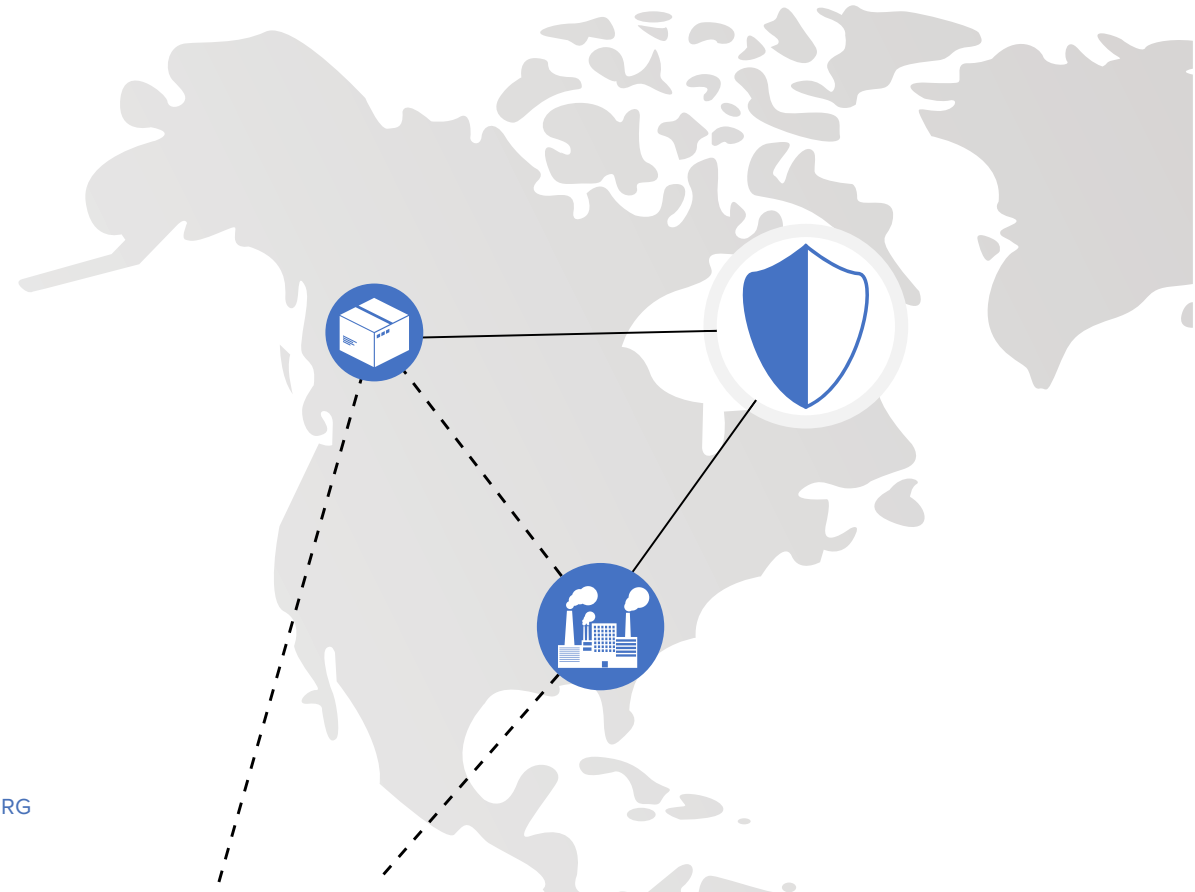
1. INTRODUCTION

Over the past few years, industry and government have continued down a path toward full digital transformation. More recently, 5G networks have enabled innovative solutions across new markets and applications. As 5G continues to advance in the marketplace, the 5G supply chain is becoming the foundational linkage to delivering assured 5G networks.

From a practical perspective, the pathway to assured 5G networks should be more appropriately viewed as progression than a binary transition. In addition, it is acknowledged that public and private networks will need to support various levels of assurance to meet customer demands and 5G application needs.

In 2019, discussions between the Alliance for Telecommunications Industry Solutions (ATIS) and the U.S. Department of Defense set the stage for the launch of ATIS' 5G Supply Chain Working Group (5G/SC WG). While it is recognized that significant focus has been placed on creating recommendations and best practices for supply chain risk management over the past few years, there is no single standards-based framework for supporting the concept of assured 5G networks. The ATIS 5G/SC initiative launched in late 2019, chaired by T-Mobile USA, Verizon, and NTIA, to address this urgent need. Over the past two years, this initiative has grown to over 50 companies, government agencies, and academic institutions, with the goal of finalizing the 5G/SC standard by the end of this year.

This paper provides a high-level overview of the current approach and framework being fully developed within the ATIS 5G/SC initiative.



2. ADDRESSING FUTURE SUPPLY CHAIN CHALLENGES

From a holistic standpoint, the 5G supply chain must be considered within the larger context of securing 5G infrastructure, which includes cybersecurity threats and supply chain vulnerabilities.

While cybersecurity threats represent an ever-increasing challenge to business, government, and consumers, securing the supply chain similarly represents an equally important challenge to the security and economic competitiveness of North America and the world.

The Interos Annual Global Supply Chain Report "reveals that global supply chain disruptions cost large companies, on average, $184 million a year and that global supply chain risk management and resilience will be the top business priority for 50% of organizations in two years' time."[1]

A study by The Economist Intelligence Unit found that up to $4 trillion in revenue may have evaporated in supply chain disruptions in 2020.[2] Although these disruptions can be attributed to many factors, including the pandemic, the economic and national security threats associated with the supply chain are becoming one of the key components of mission-critical applications across industry and government.

To this end, a significant number of public-private collaborative efforts have been launched to address ICT Supply Chain Risk Management (SCRM). Most significantly, the Cybersecurity and Infrastructure Security Agency (CISA) launched the ICT SCRM Task Force in October 2018 to provide advice and recommendations for assessing and managing risks associated with the ICT Supply Chain. The ICT SCRM Task Force published several reports covering threat scenarios, impacts, and mitigating controls to threats and the related application to products and services.

The ATIS 5G/SC WG is now taking the next step in leveraging the important work of industry and government collaboratives on ICT SCRM to develop a framework and associated standards that will lead to assured 5G networks. 5G represents the current runway of mobile technology deployments that will span the decade. A secure supply chain will play a pivotal role in addressing the complexities of 5G deployment in new markets, IoT applications, public and private networks, and a wide range of government applications.

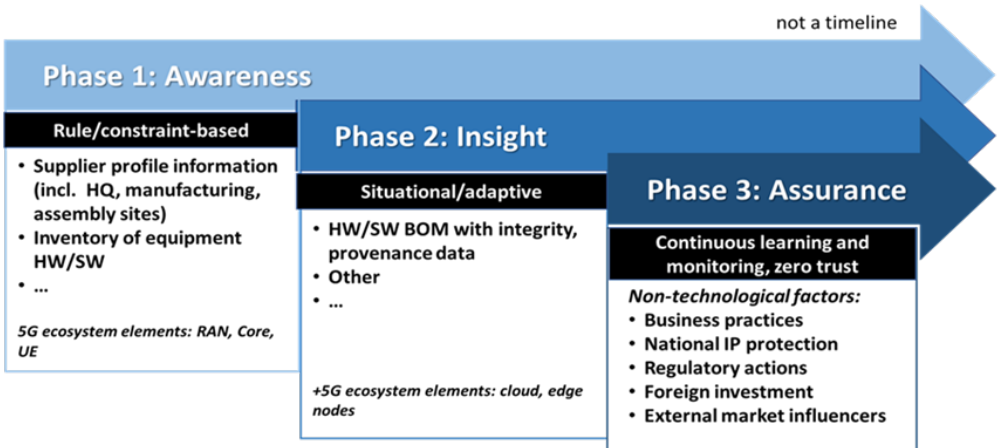
1 Interos Annual Global Supply Chain Report, https://www.interos.ai/resources/global-supply-chain-report/, June 2021

2 The Economist Intelligence Unit report, https://www.gep.com/clp/the-business-costs-of-supply-chain-disruption/, June 2021

3. EVOLUTION TO ASSURED 5G NETWORKS

As we progress through the next decade, 5G will continue to offer impactful solutions and create new opportunities for innovative applications across many industry sectors and government needs. Correspondingly, supply chain assurance must progress to meet the complexity of new applications and to combat an increasing level of threats to network assurance and resiliency.

The evolution to assured 5G networks can best be viewed as a progression from awareness to insight and ultimately to assurance through (1) the application of rules (2) the collection of situational data, and (3) the movement to continuous learning and zero trust processes.



Reaching an assurance level is not a destination, but a progression in light of a constantly changing and evolving threat environment.

Source: U.S. Department of Defense

The first phase on the path toward assurance is awareness. It includes a thorough understanding of inventory of components used in the supply chains, as well as the life cycle processes used in design, inbound supply, build, distribution, integration, operation, and post-operation functions across the flow of components in the supply chain.

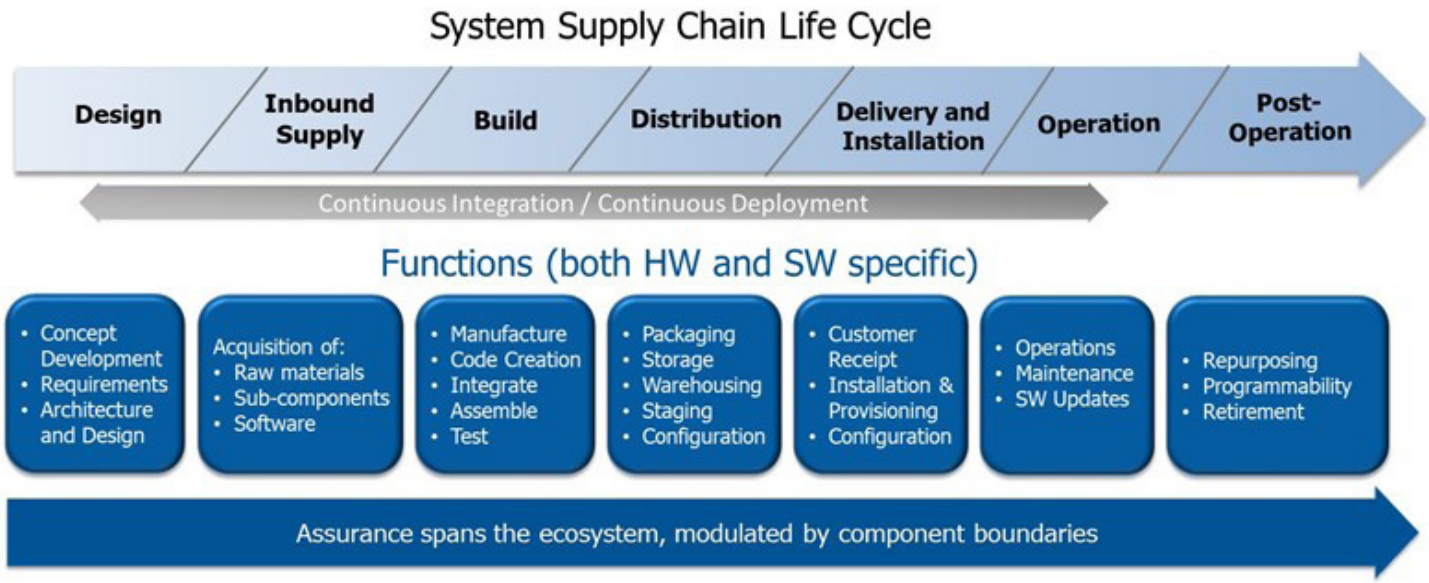
The second phase is insight. It includes the management of information life cycles that capture key characteristics of both software and hardware to manage components and assist in verifying the authenticity and integrity of components and tracking vulnerabilities. This phase leverages structures such as Software Bill of Materials (SBOM), Hardware Root of Trust (HRoT) and other mechanisms related to component provenance.

The third phase is assurance. It requires a broader focus beyond the individual components that make up the end system to include the global business market and regulatory factors.

4. 5G SUPPLY CHAIN LIFE CYCLE

The ecosystem surrounding 5G supply chain is a complex set of relationships between acquirers, integrators, and suppliers. Depending on the circumstances, entities can operate at two or more of these levels.

The following diagram provides an end-to-end view of the 5G supply chain ecosystem and its related lifecycle. It is important to note that these stages are not intended as sequential steps. Instead, they are a continuous flow of supply chain functions and processes across the integration and deployment of an assured 5G network, which may include components, sub-components, software, and hardware elements.



The ATIS 5G/SC WG has adopted an intentionally broad view of supply chain that spans from design to post-operation. This view recognizes that threats are present for each of the above life cycle functions and should be considered for any supply chain mitigation plan.

It is also important to note that both the components and associated metadata have a life cycle. Understanding the functions that exist within each stage of the supply chain life cycle enables a deep assessment of the threats, controls, and requirements that are associated with each component that flows across the supply chain cycle.

5. KEY 5G SUPPLY CHAIN ATTRIBUTES

An attribute is a defining quality of an asset (hardware component, module, system, software) and consequently reflects the asset's attackable characteristics. Attributes should exhibit characteristics of completeness and independence. All attacks will generally map to one or more attributes.

The following 5G/SC attributes have been adopted and applied to the supply chain flow:

- Integrity
- Authenticity
- Provenance
- Availability
- Confidentiality

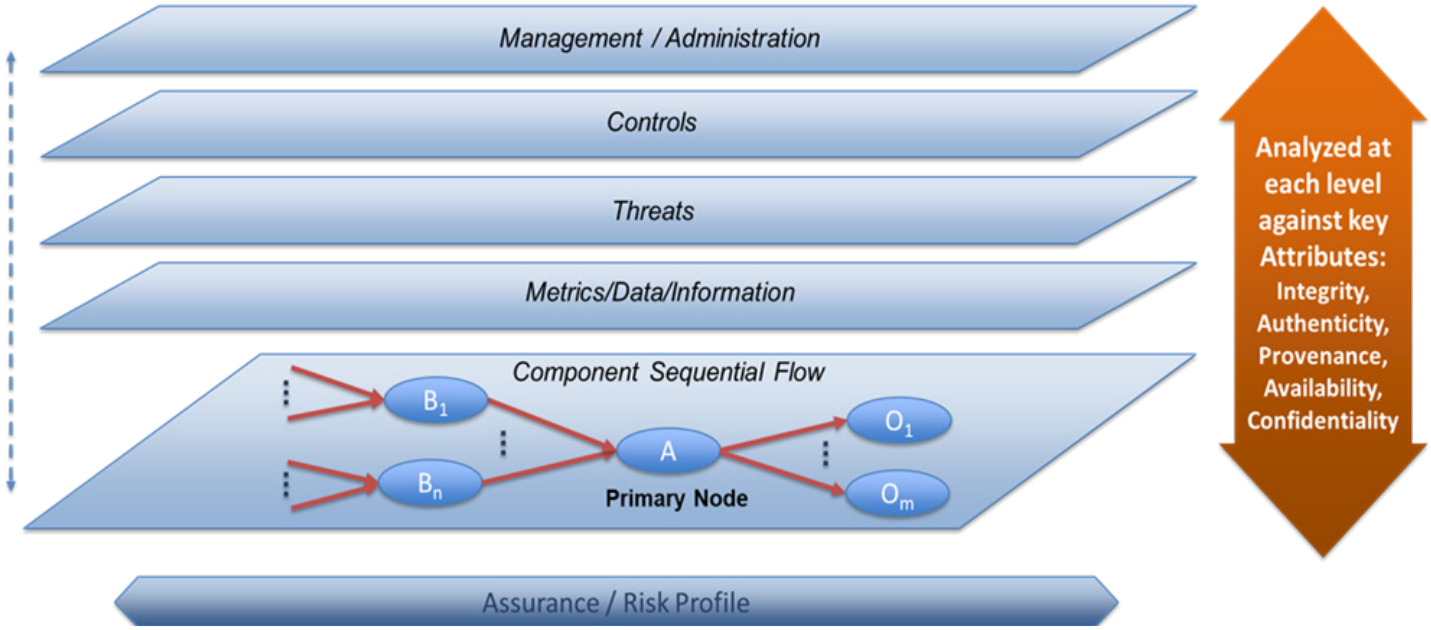
These attributes relate to both components and systems of components as well as the data security of the information associated with the supply chain, and are described as follows:

ATTRIBUTE	**As Applied to Components**	**As Applied to Data Security**
Integrity	Meets stated requirements with no undocumented capabilities (i.e., it is what it's supposed to be, and nothing else).	Data has not been modified by unauthorized identities.
Authenticity	Created/service performed by known documented entities, touched only by whom it was supposed to have been touched by.	Reflecting the property of being verifiably genuine (i.e., associated with the identity of the data and who has access to the data).
Provenance	A record of creation of an object and its components, and every hand that has touched it.	N/A
Availability	It is available when needed/as planned.	Timely and reliable authorized access to uncompromised data.
Confidentiality	The asset can only be accessed (touched, seen, or used) by authorized, authenticated identities.	Ensuring that data associated with a component is protected from unauthorized use (read/modify).

6. A LAYERED 5G SUPPLY CHAIN MODEL

The 5G/SC WG undertook the organic development of a 5G supply chain framework that encompasses the previously described component flow model. It also includes a layered approach that assesses threats and vulnerabilities and applies the appropriate controls at each level of the model architecture.

The following diagram provides a multi-layered view that can be applied to any 5G supply chain component, sub-component, or software, analyzing each stage of the flow with respect to the key attributes identified earlier in this document.

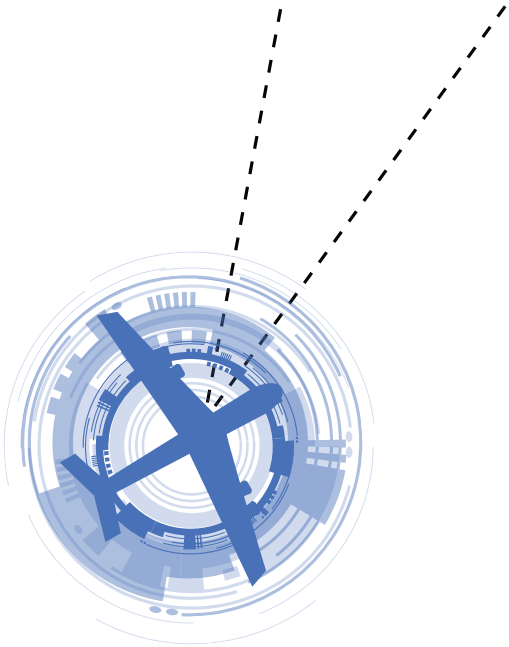


The Metrics, Data and Information layer is associated with the target component/service/function used to support the process steps required for assurance. This includes capabilities such as:

- Identity (signatures, serial numbers, certificates of authenticity)
- Integrity (e.g., using cryptographic hashes and signatures)
- Characteristics (critical information, programmability level, policy compliance)
- History of activity (shipping/tracking information, provenance-related information)
- Vulnerability tracking (where the component is deployed and what vulnerabilities exist)

The Threats layer contains a list of threats identified and categorized by risk. Controls and management techniques can then be applied to mitigate threats that pose a serious risk of impact based on the end application/service.

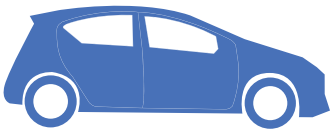
Threats may include, for example:



- Software vulnerabilities
- Code-signing issues
- Hijacked update processes
- Open source with malware insertion
- Compromised (embedded) credentials and weak cryptography
- Hardware vulnerabilities
- Tampering/modification
- Programmability vulnerabilities
- Substitution

The Controls layer includes the specific tests, verifications, audits, and other functions to provide assurance in mitigating a threat relative to one or more attributes. Typical controls may include, for example:

- Product bar code scans
- Physical security of facilities and packaging (e.g., locks and enclosures)
- Integrity tests of HW/SW via HRoT Verification and other means
- Encryption/code signing
- Software scans to identify potential malware
- Inspection
- Tracking with documentation
- Verification of certifications, standards, and compliance requirements



The Management and Administration layer includes the supply chain process aspects used to help assure the supply chain's security. This includes vendor management and contracting:

- Utilization of preferred vendor lists
- Enforcement of vendor diversity
- Contractual obligations to ensure that vendors meet specific supply chain standards and/or use specific security best practices and processes
- Contractual enforcement provisions (e.g., required audits, liquidated damages)

7. PROGRESSING TO CONTROLS AND REQUIREMENTS

The ATIS 5G/SC WG is now transitioning its work to the development of detailed controls and requirements across the supply chain lifecycle.

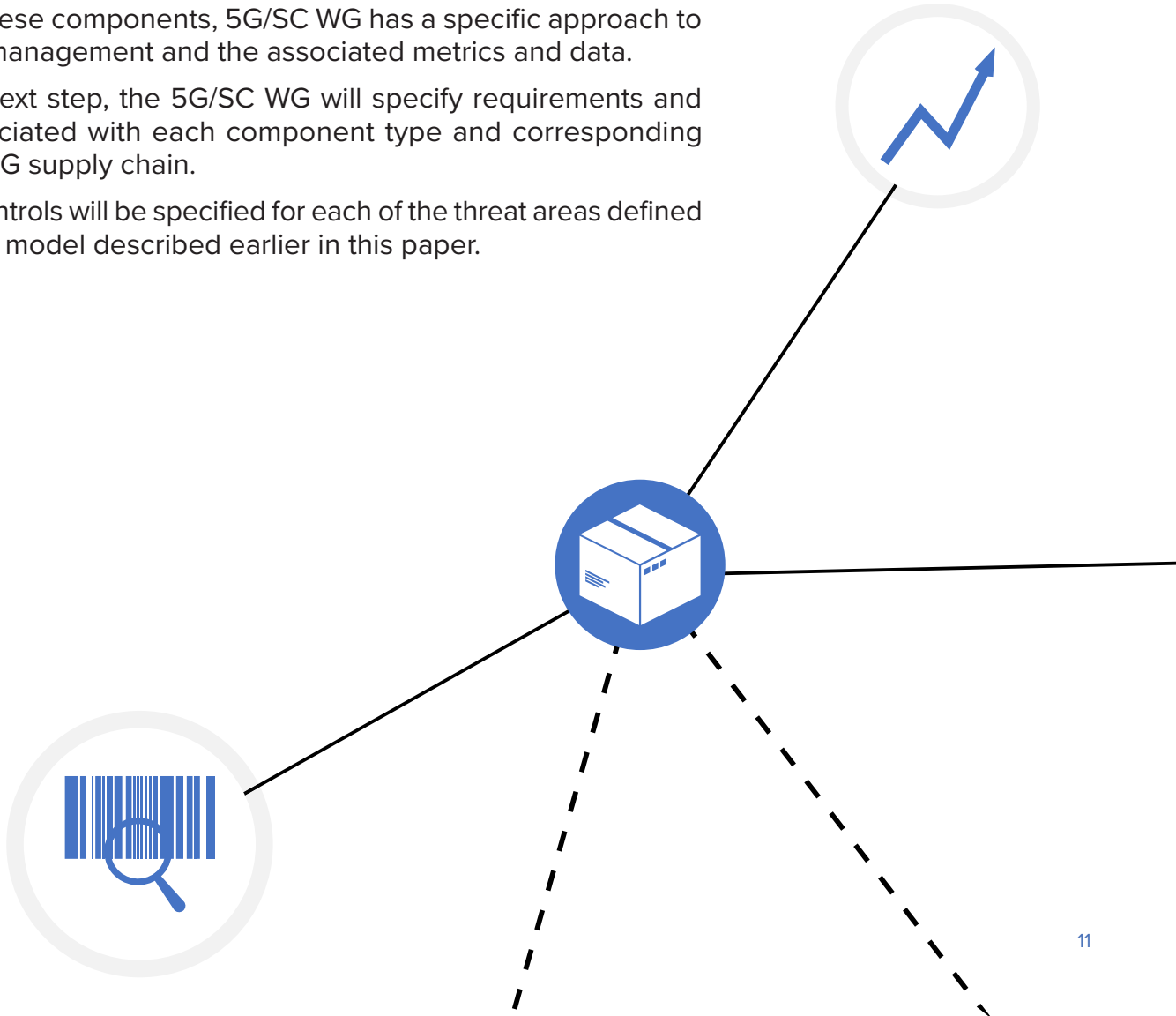
In order to develop the detailed requirements associated with different types of supply chain components, the 5G/SC WG has defined four types:

- Open-source software
- Proprietary software
- Software-controlled hardware
- Other hardware

For each of these components, 5G/SC WG has a specific approach to vulnerability management and the associated metrics and data.

As a critical next step, the 5G/SC WG will specify requirements and controls associated with each component type and corresponding stage of the 5G supply chain.

In addition, controls will be specified for each of the threat areas defined in the layered model described earlier in this paper.



8. SUMMARY

Over the past few years, supply chain security has been recognized by both industry and government as one of the key factors that will impact infrastructure resiliency and drive future economic competitiveness. As the ICT sector continues to deploy innovative 5G technology solutions across public and private communications networks, as well as adjoining industries, securing the supply chain becomes a key imperative.

The ATIS 5G/SC WG represents a collaboration between the private sector and North American governments to develop a flexible set of 5G supply chain standards that can progress with greater awareness, insight, and assurance. Ultimately, the ATIS 5G/SC standard can be applied to a range of assurance levels that represent the specific application-driven ecosystem.

It is expected that the 5G/SC WG will complete its development of this standard by the end of 2021 and will move to publication in early 2022.

Additional companies, academic institutions, and government agencies are invited to join this effort and contribute to the final development of the ATIS 5G supply chain standard.

For more information please see: **https://www.atis.org/**.