Software Supply Chain Risks That May Need to be Addressed

MITRE's System of Trust™

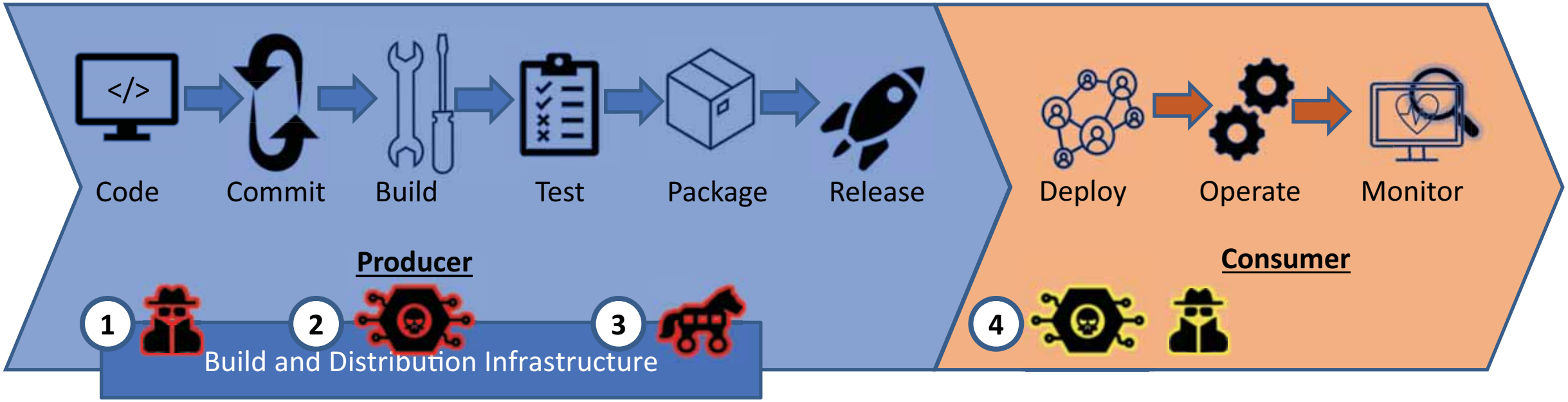
Robert Martin
Senior Software and Supply Chain Assurance Principal Engineer
Cyber Solutions Innovation Center
MITRE Labs

Presenting at the ITU Workshop on "Zero Trust and Software Supply Chain Security"
Session 2: Need, security issues, threats and controls for software supply chain security.

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD™

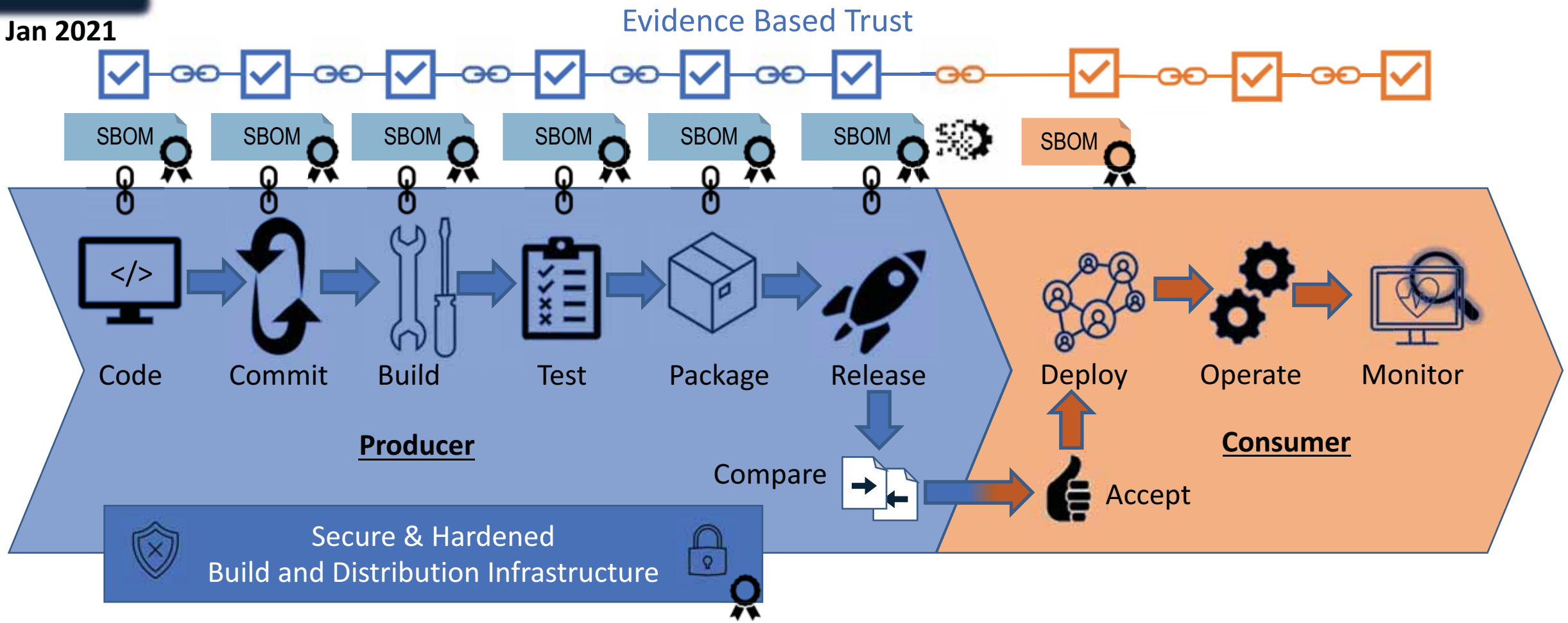
Software Supply Chain Attack (a.k.a SolarWinds)

1. Preparatory compromises at SolarWinds date back to **October 2019**. (Refs 11 & 12)
2. At some point there was a compromise of the build environment itself.
3. Malicious code sent in SolarWinds updates released between March and at least **June 2020**. (Refs 32 & 33)
4. Approximately 18,000 organizations receive the tainted updates and may have been targeted and impacted.



Software Supply Chain Integrity

Jan 2021

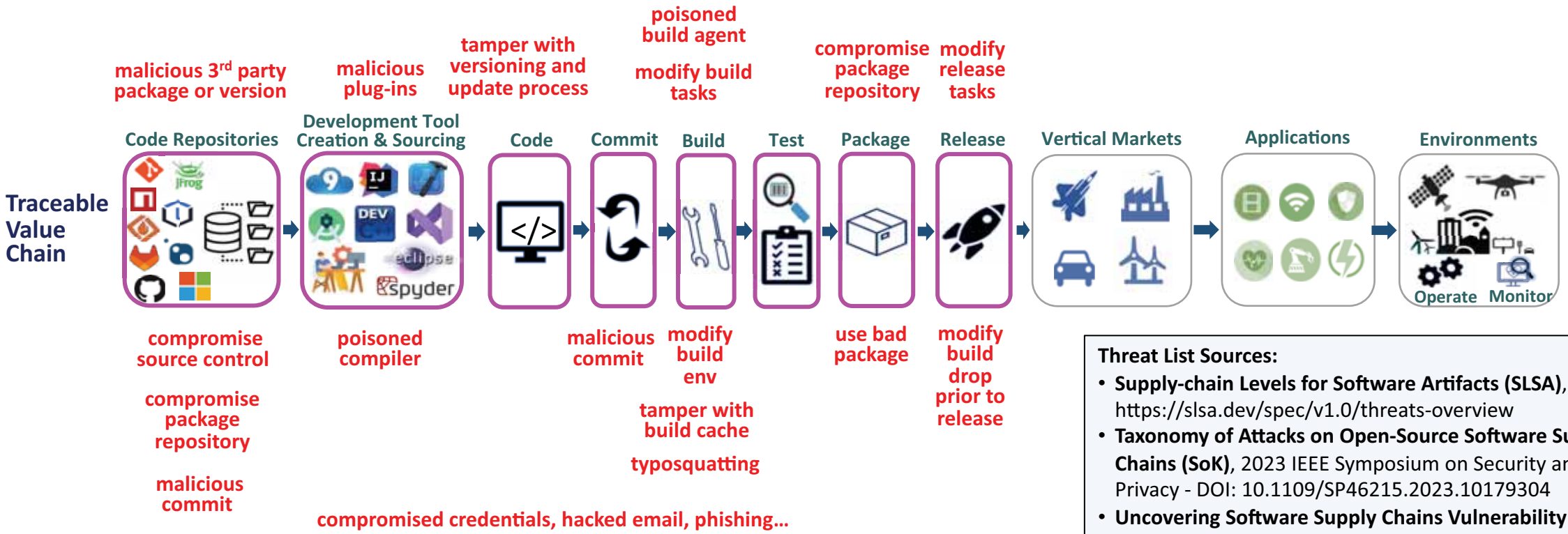


https://www.mitre.org/sites/default/files/publications/pr-21-0278-deliver-uncompromised-securing-critical-software-supply-chains.pdf

Software Supply Chain Integrity, Transparency & Trust

SW Parts & Tooling Ecosystem | Software Product Ecosystem | Edge Ecosystem

Software Supply Chain Risks (Hazards and Threats)*



Threat List Sources:

- **Supply-chain Levels for Software Artifacts (SLSA)**, https://slsa.dev/spec/v1.0/threats-overview
- **Taxonomy of Attacks on Open-Source Software Supply Chains (SoK)**, 2023 IEEE Symposium on Security and Privacy - DOI: 10.1109/SP46215.2023.10179304
- **Uncovering Software Supply Chains Vulnerability: A Review of Attack Vectors, Stakeholders, and Regulatory Frameworks**, DOI: 10.1109/COMPSAC57700.2023.00281

* See MITRE's System of Trust repository of potential supply chain risks (SoT.MITRE.ORG)

MITRE

System of Trust (SoT)

"What Supply Chain Risks to Manage?"

SoT - a strategic, widely-adoptable, holistic, data-driven analysis platform to assess supply chain security risks

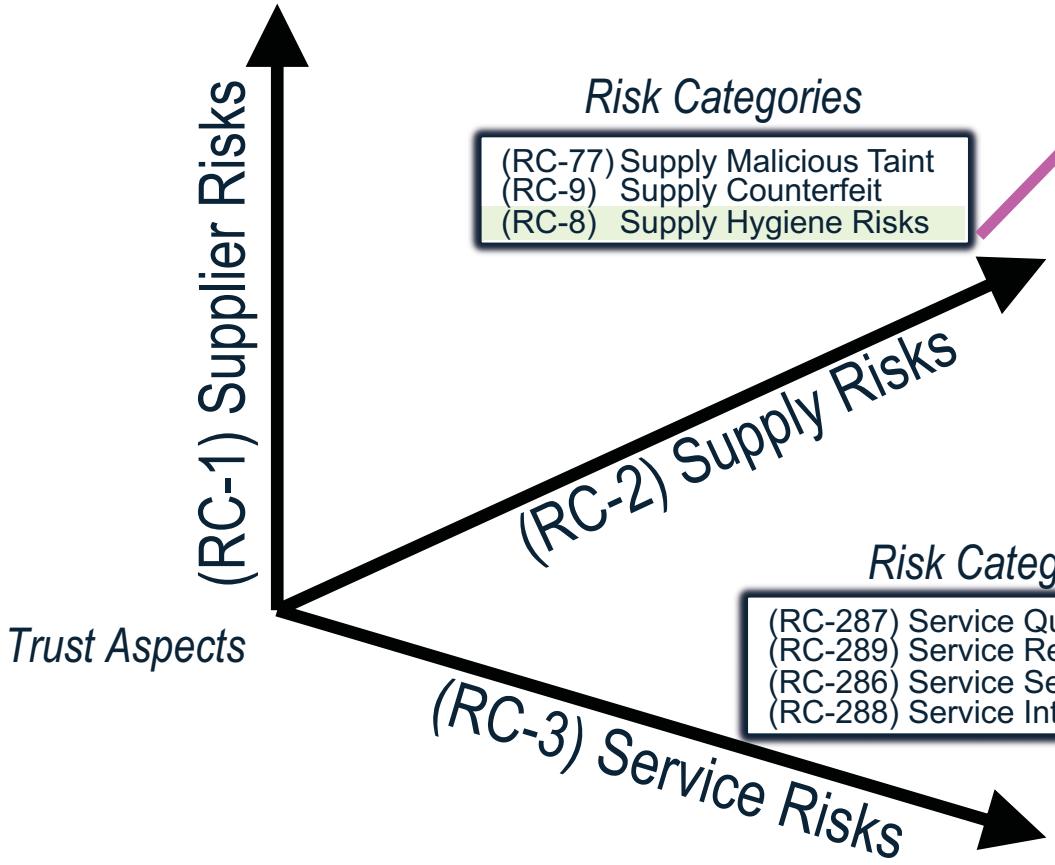
Address Chaos, Align & Organize

Simplify, Tailor & Use

Basis of Trust

Risk Categories

(RC-13) Supplier Financial Stability Risks
(RC-76) Supplier Organizational Security Risks
(RC-4) Supplier Susceptibility
(RC-20) Supplier Quality Culture Risks
(RC-105) Supplier Organizational Effectiveness Risks
(RC-7) Supplier Ethical Risks
(RC-6) Supplier External Influences



Risk Categories

(RC-77) Supply Malicious Taint
(RC-9) Supply Counterfeit
(RC-8) Supply Hygiene Risks

Risk Categories

(RC-287) Service Quality Risks
(RC-289) Service Resilience Risks
(RC-286) Service Security Risks
(RC-288) Service Integrity Risks

(RC-8) Supply Hygiene Risks

(RC-201) Supply (product) Quality Risks
(RC-213) Supply (product) Security Risks
(RC-214) Supply (product) Resilience Risks

(RC-213) Supply (product) Security Risks

(RC-518) Software supply (product) security process risks
(RC-519) Software supply (product) security requirements risks
(RC-520) Software supply (product) architecture and design security risks
(RC-521) Software supply (product) coding language risks
(RC-522) Software supply (product) code analysis risks
(RC-523) Software supply (product) security testing risks
(RC-524) Software supply (product) secure build risks
(RC-525) Software supply (product) secure integration and deployment risks
(RC-526) Software supply (product) secure update risks
(RC-527) Software supply (product) pedigree and provenance risks
(RC-528) Third party supply (product) component risks

(RC-528) Third party supply (product) component risks

(RF-113) Software supply (product) includes components that were known to have exploitable vulnerabilities at the time it was in development
(RC-529) Open source software risks for software supply (product)
(RF-743) Insufficient security vetting of third party software supply (product) components

MITRE

MITRE Supply Chain Security System of Trust Risk Areas* **

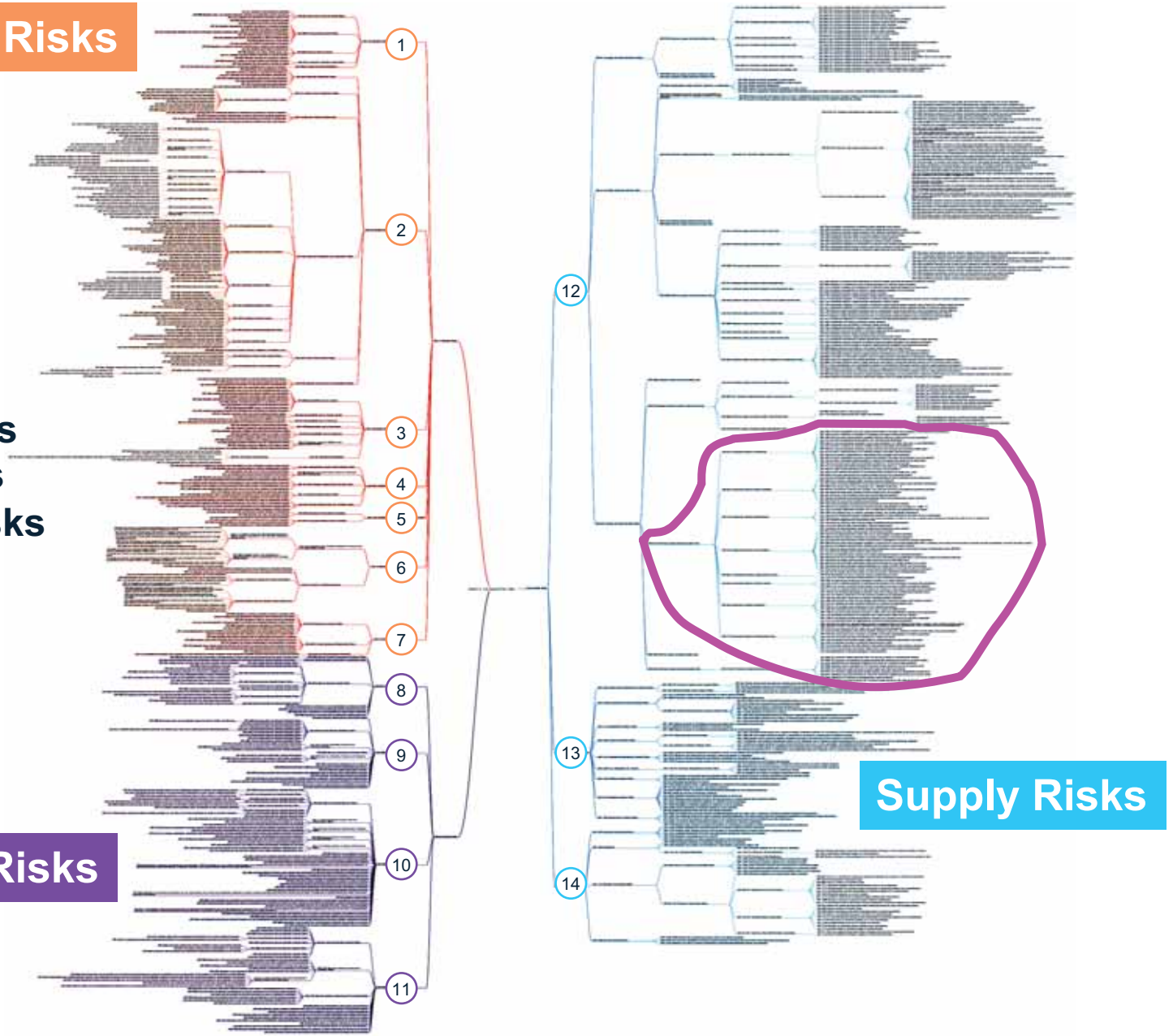
Supply Chain Risks														
(RC-1) Supplier Risks							(RC-2) Supply Risks			(RC-3) Service Risks				
(RC-13) Supplier Financial Stability Risks	(RC-76) Supplier Organizational Security Risks	(RC-4) Supplier Susceptibility	(RC-20) Supplier Quality Culture Risks	(RC-105) Supplier Organizational Effectiveness Risks	(RC-7) Supplier Ethical Risks	(RC-6) Supplier External Influences	(RC-77) Supply Malicious Taint	(RC-9) Supply Counterfeit	(RC-8) Supply Hygiene Risks	(RC-287) Service Quality Risks	(RC-289) Service Resilience Risks	(RC-286) Service Security Risks	(RC-288) Service Integrity Risks	
(RC-257) Short-term Financial Health Risks	(RC-403) Technical Operations Risks	(RC-22) Susceptibility due to Location	(RC-630) Subcontractor Supply Chain Hygiene Risks	(RC-538) Structural & Operational Instability	(RC-15) Association with Foreign Intelligence Service (FIS) or Foreign Military Entity	(RC-5) Ownership and Control Risks	(RC-155) Supply Chain Management Integrity Risks	(RC-127) Unsanctioned Manufacturing	(RC-214) Supply (product) Resilience Risks	(RC-563) Service Quality Infrastructure Pedigree Risks	(RC-598) Service Infrastructure Redundancy Risks	(RC-294) Service Specific Security Risks	(RC-301) Service Specific Integrity Risks	
(RC-256) Financial Stewardship Risks	(RC-441) Cyber Threat Intelligence Risks	(RC-25) Susceptibility due to Industry Sector	(RC-82) Supplier has Performance Issues on Contracts with other Companies	(RC-537) Geographical/Geopolitical Instability	(RC-26) Pattern of Criminal Behavior	(RC-534) Foreign Business Relationship Risks	(RC-149) Manufacturing Process Integrity Risks	(RC-126) Mislabeling	(RC-213) Supply (product) Security Risks	(RC-562) Service Quality Infrastructure Provenance Risks	(RC-599) Service Infrastructure Diversity Risks	(RC-11) Remote/Virtual Access to Service Infrastructure Risks	(RC-576) Service Integrity Infrastructure Pedigree Risks	
(RC-260) Adverse Market Factors	(RC-16) Security Training Deficiencies	(RC-21) Susceptibility due to Personnel	(RC-18) Subcontractor Supply Chain Security Risks			(RC-536) Adverse Corporate Influences	(RC-154) Geopolitical Integrity Risks	(RC-118) Technical Authenticity Risks	(RC-201) Supply (product) Quality Risks	(RC-300) Service Specific Quality Risks		(RC-296) Service Security Infrastructure Pedigree Risks	(RC-575) Service Integrity Infrastructure Provenance Risks	
(RC-258) Long-term Financial Health Risks	(RC-346) Security Capabilities and Operations Risks	(RC-448) Susceptibility due to Espionage	(RC-19) Internal Quality Control Risks				(RC-153) Functional Integrity Risks	(RC-128) Copycat Manufacturing		(RC-302) Service Specific Reliability Risks		(RC-295) Service Security Infrastructure Provenance Risks		
(RC-262) Foreign Financial Obligations	(RC-434) Cyber Threat Activity Risks	(RC-24) Susceptibility due to Customers	(RC-632) Internal SCRM Policy and Practices Risks				(RC-151) Logistics/Transportation Integrity Risks			(RC-587) Service Reliability Infrastructure Provenance Risks		(RC-10) Physical Access to Service Infrastructure Risks		
	(RC-400) Security Governance and Compliance Risks	(RC-23) Technical Susceptibility					(RC-152) Poor Reputation for Integrity			(RC-588) Service Reliability Infrastructure Pedigree Risks				
							(RC-150) Facilities Integrity Risks							
							(RC-54) Packaging Integrity Risks							
							(RC-156) Maintenance Integrity Risks							

MITRE's Supply Chain Security System of Trust™ https://sot.mitre.org/

* Supply Chain Security Top 75 Risk Areas Levels 1-3
** System of Trust Expanding to Pharma, Food, and other types of Products

MITRE

Supplier Risks

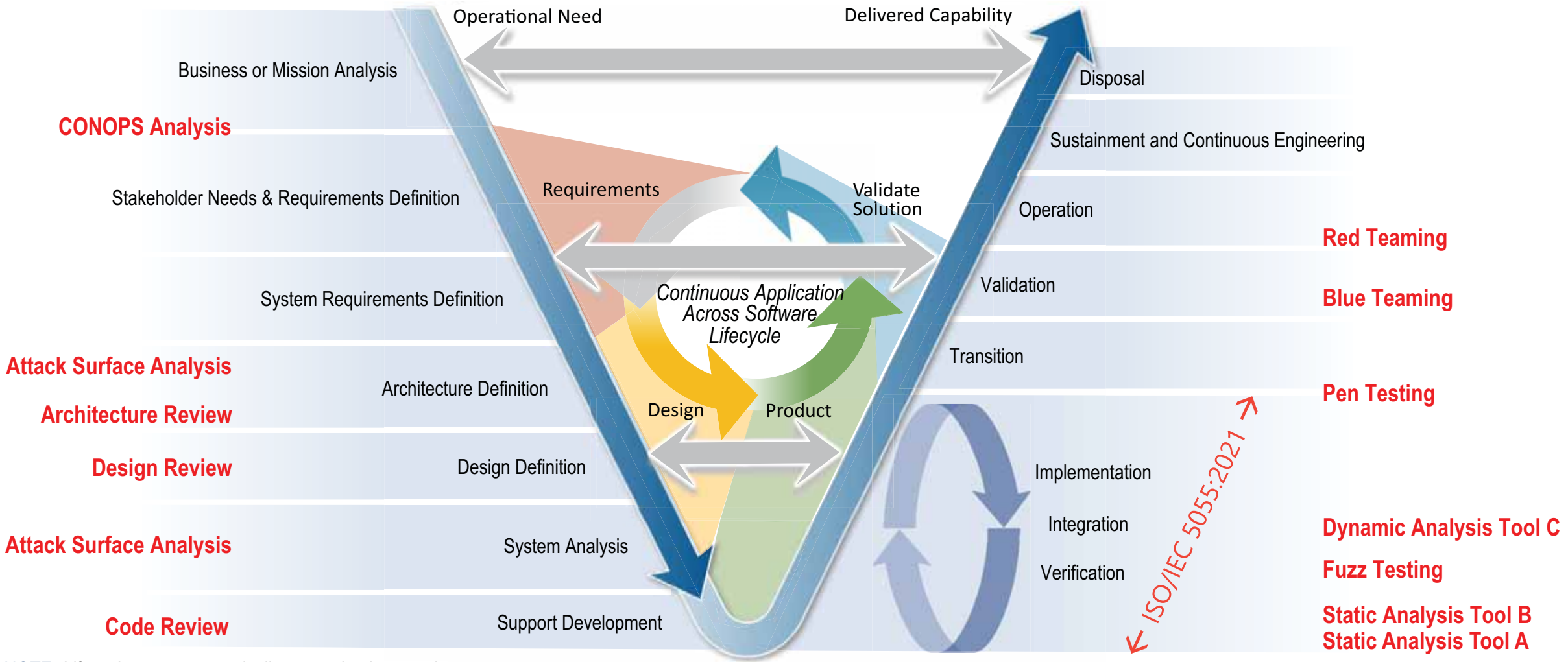


14 top-level risk categories
214 detailed risk categories
642 specific measurable risks

Service Risks

Supply Risks

Software Development and Assurance Evidence Sources



NOTE: *Lifecycle processes typically occur simultaneously, **not** in sequence; see ISO/IEC 15288 & 12207*

NOTE: *Implementation, Integration & Verification are often performed continuously & simultaneously with the aid of Integrated Development Environments (IDEs) & other tools.*

Figure 3-2 from "Software Trustworthiness Best Practices," 2020, https://www.iiconsortium.org/pdf/Software_Trustworthiness_Best_Practices_Whitepaper_2020_03_23.pdf

SBOM Definition

NTIA Minimal Elements (EO 14028)

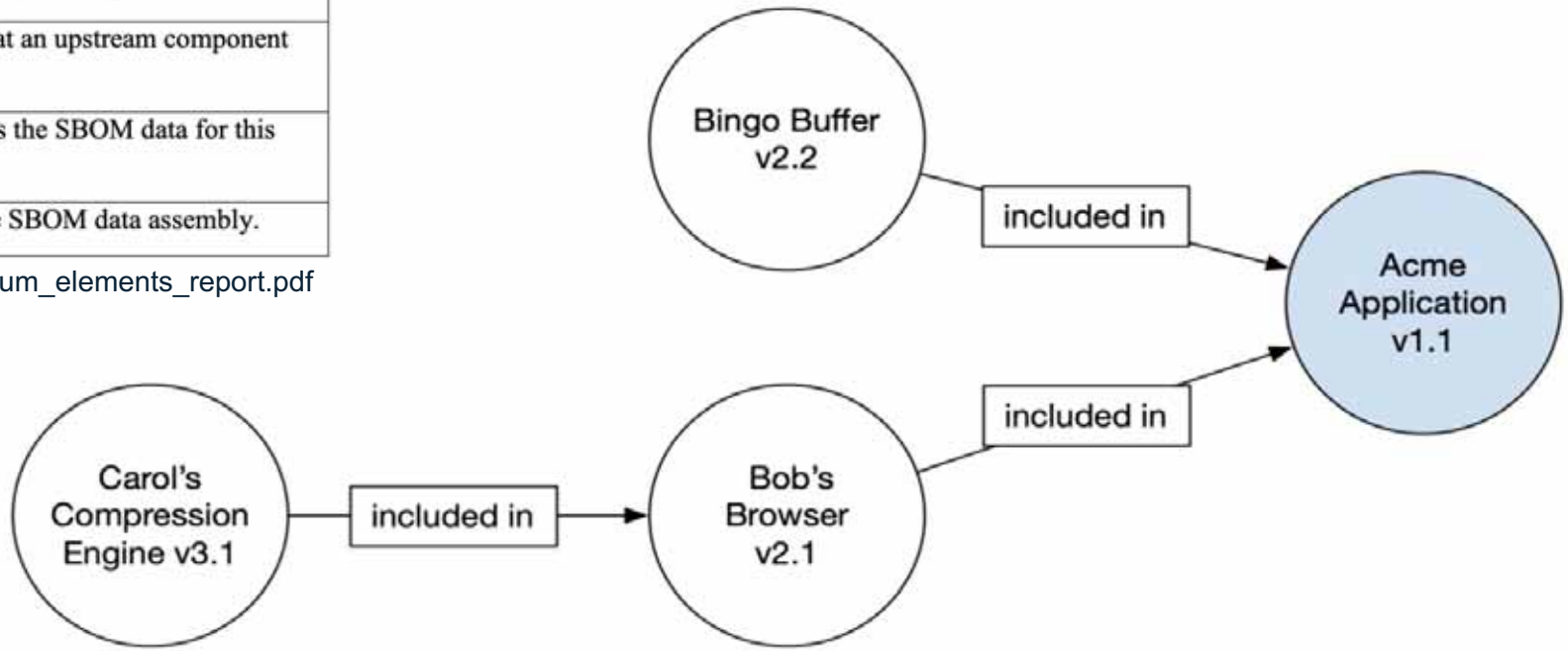
Data Field	Description
Supplier Name	The name of an entity that creates, defines, and identifies components.
Component Name	Designation assigned to a unit of software defined by the original supplier.
Version of the Component	Identifier used by the supplier to specify a change in software from a previously identified version.
Other Unique Identifiers	Other identifiers that are used to identify a component, or serve as a look-up key for relevant databases.
Dependency Relationship	Characterizing the relationship that an upstream component X is included in software Y.
Author of SBOM Data	The name of the entity that creates the SBOM data for this component.
Timestamp	Record of the date and time of the SBOM data assembly.

https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf

Minimum Elements	
Data Fields	Document baseline information about each component that should be tracked: Supplier, Component Name, Version of the Component, Other Unique Identifiers, Dependency Relationship, Author of SBOM Data, and Timestamp.
Automation Support	Support automation, including via automatic generation and machine-readability to allow for scaling across the software ecosystem. Data formats used to generate and consume SBOMs include SPDX, CycloneDX, and SWID tags.
Practices and Processes	Define the operations of SBOM requests, generation and use including: Frequency, Depth, Known Unknowns, Distribution and Delivery, Access Control, and Accommodation of Mistakes.

https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf

SPDX (Linux Foundation - Free ISO/IEC 5952:2022)
CycloneDX (OWASP Project)
SWID



Source: https://www.ntia.gov/files/ntia/publications/ntia_sbom_framing_2nd_edition_20211021.pdf

MITRE

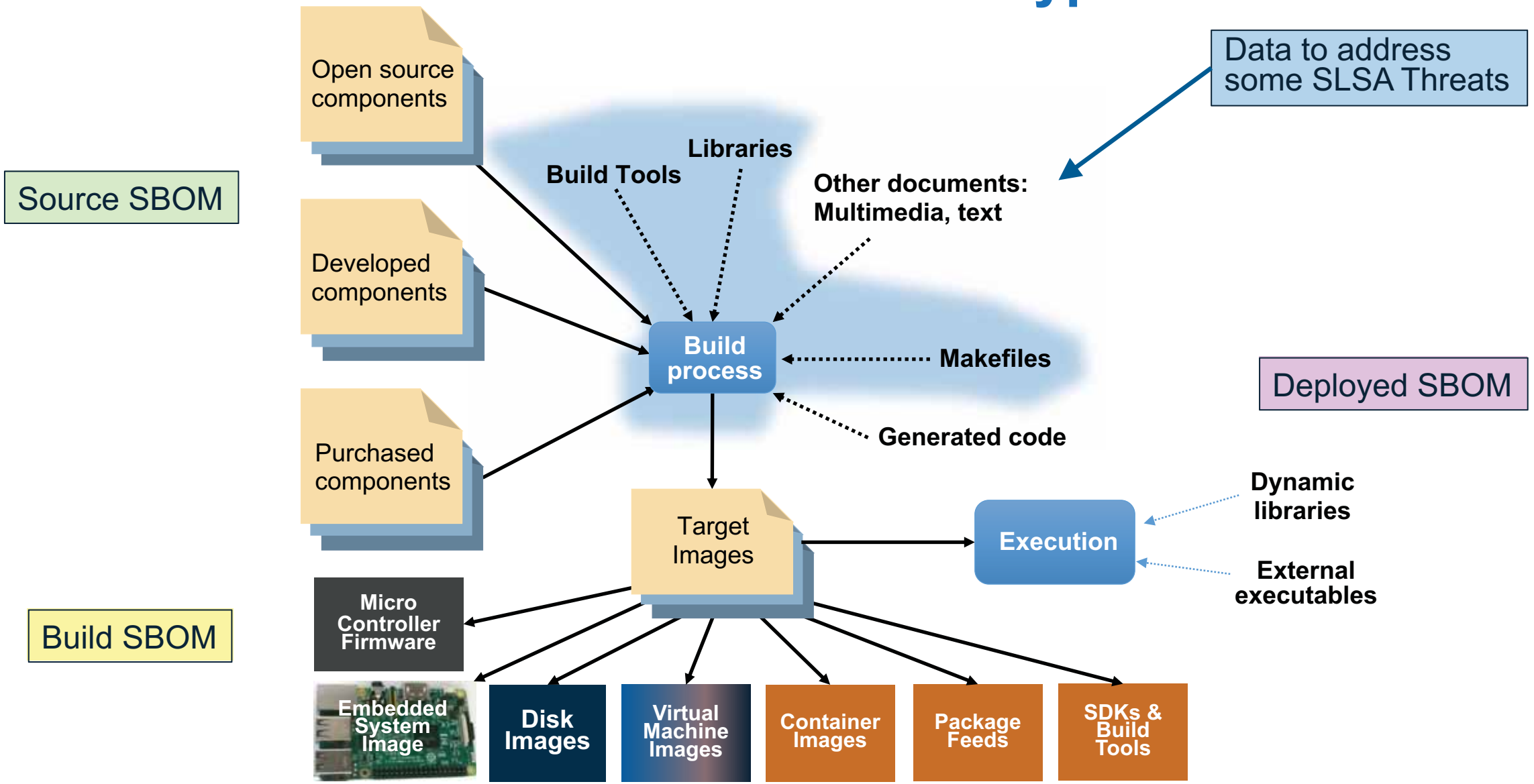
From the Community-led Working Group on SBOM Tooling and Implementation, facilitated by Cybersecurity and Infrastructure Security Agency [cisa.gov/sbom]

Table 1: SBOM Type Definition and Composition

SBOM Type	Definition	Data Description
Design	SBOM of intended design of included components (some of which may not exist) for a new software artifact.	Typically derived from a design specification, RFP, or initial concept.
Source	SBOM created directly from the development environment, source files, and included dependencies used to build an product artifact.	Typically generated from software composition analysis (SCA) tooling, with manual clarifications.
Build	SBOM generated as part of the process of building the software to create a releasable artifact (e.g., executable or package) from data such as source files, dependencies, built components, build process ephemeral data, and other SBOMs.	Typically generated as part of a build process. May consist of integrated intermediate Build and Source SBOMs for a final release artifact SBOM.
Analyzed	SBOM generated through analysis of artifacts (e.g., executables, packages, containers, and virtual machine images) after its build. Such analysis generally requires a variety of heuristics. In some contexts, this may also be referred to as a "3rd party" SBOM.	Typically generated through analysis of artifacts by 3rd party tooling.
Deployed	SBOM provides an inventory of software that is present on a system. This may be an assembly of other SBOMs that combines analysis of configuration options, and examination of execution behavior in a (potentially simulated) deployment environment.	Typically generated by recording the SBOMs and configuration information of artifacts that have been installed on systems.
Runtime	SBOM generated through instrumenting the system running the software, to capture only what is loaded and executing in memory, as well as external call-outs or dynamically loaded components. In some contexts, this may also be referred to as an "Instrumented" or "Dynamic" SBOM.	Typically generated from tooling interacting with a system to record the artifacts present in a running environment and/or that have been executed.

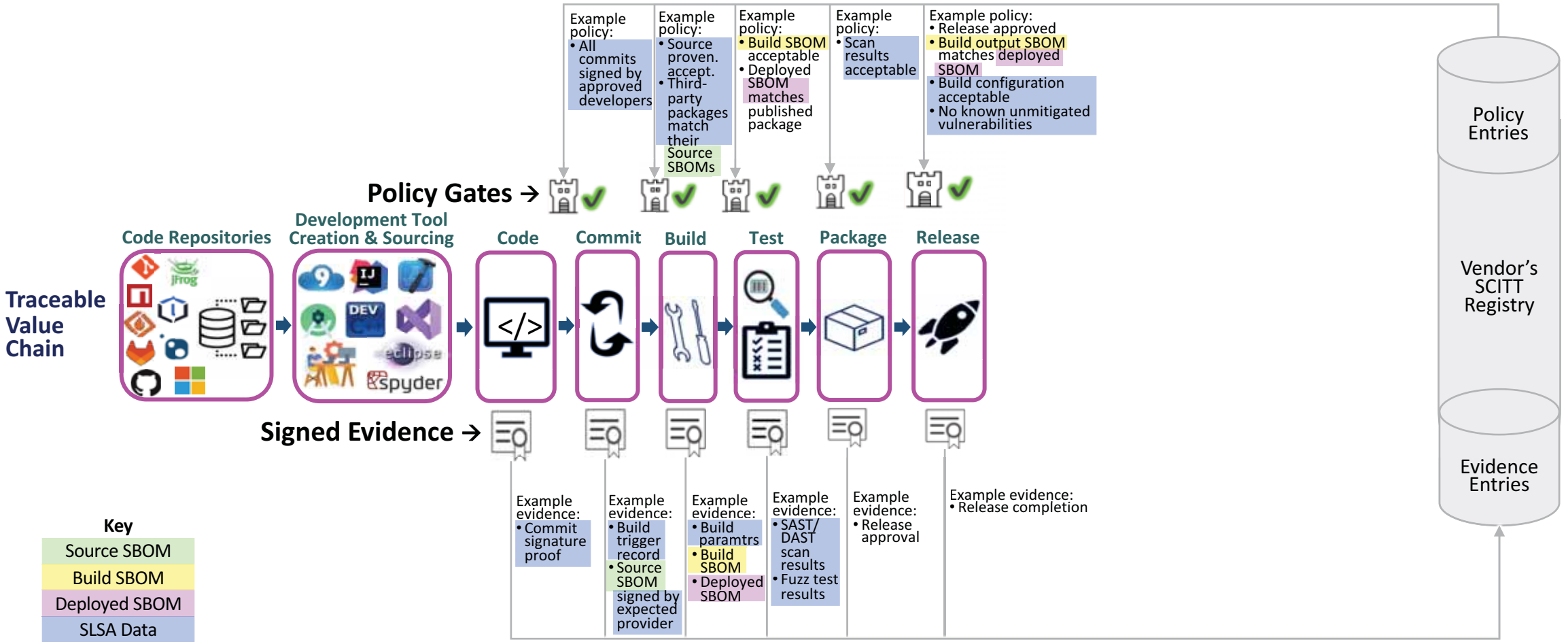
MITRE

Software Bill of Materials Types



Software Supply Chain Integrity, Transparency & Trust

SW Parts & Tooling Ecosystem | Software Product Ecosystem | Edge Ecosystem



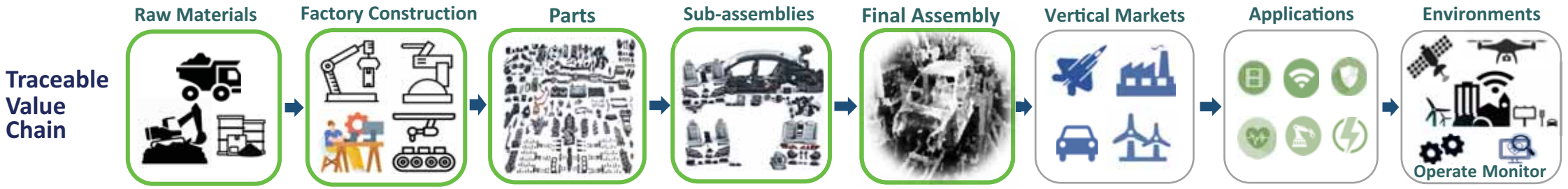
Example of the IETF SCITT in SW Development

MITRE

Auto Supply Chain Integrity, Transparency & Trust

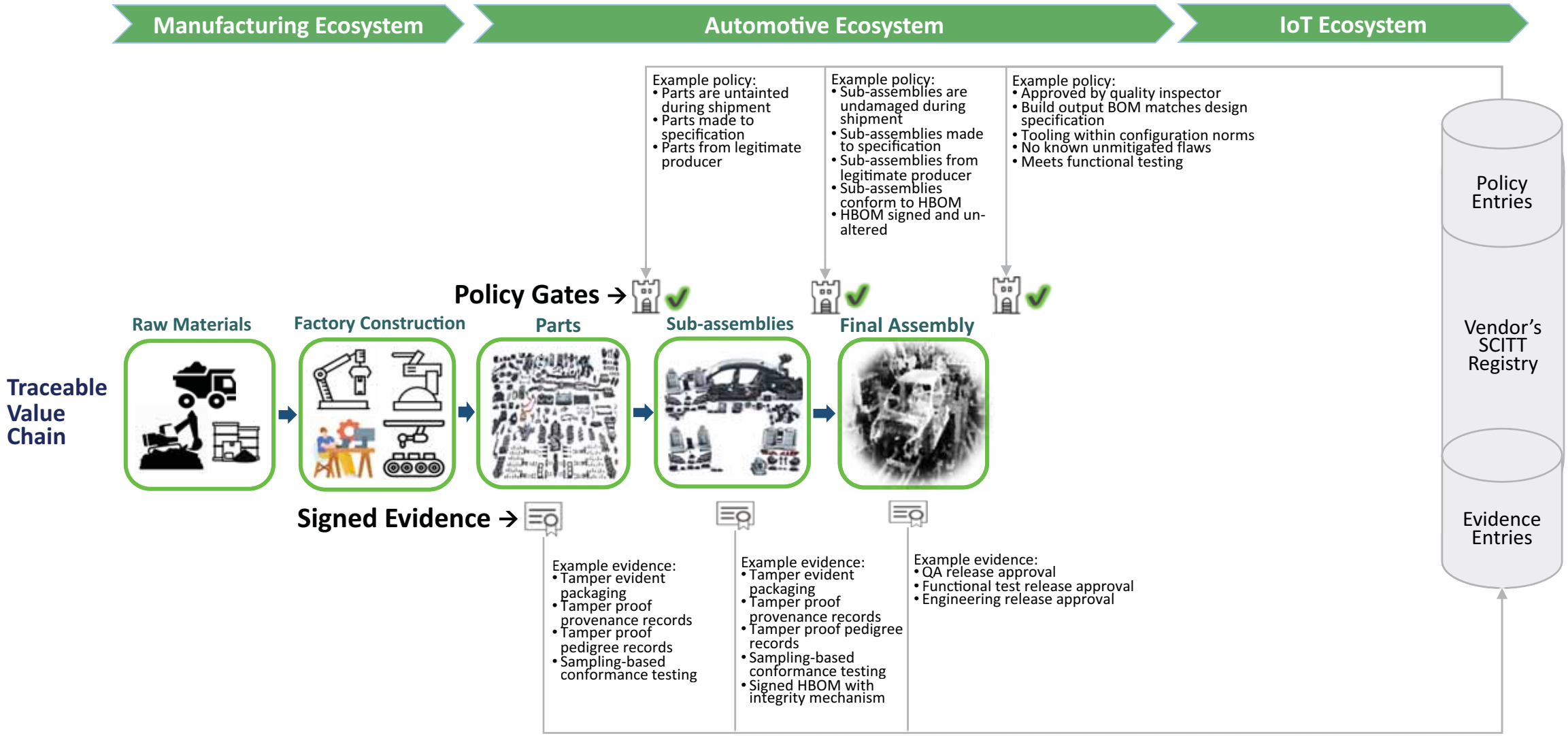
Manufacturing Ecosystem | Automotive Ecosystem | IoT Ecosystem

Automotive Supply Chain Risks (Hazards and Threats)*



* See MITRE's System of Trust repository of potential supply chain risks (SoT.MITRE.ORG)

Auto Supply Chain Integrity, Transparency & Trust



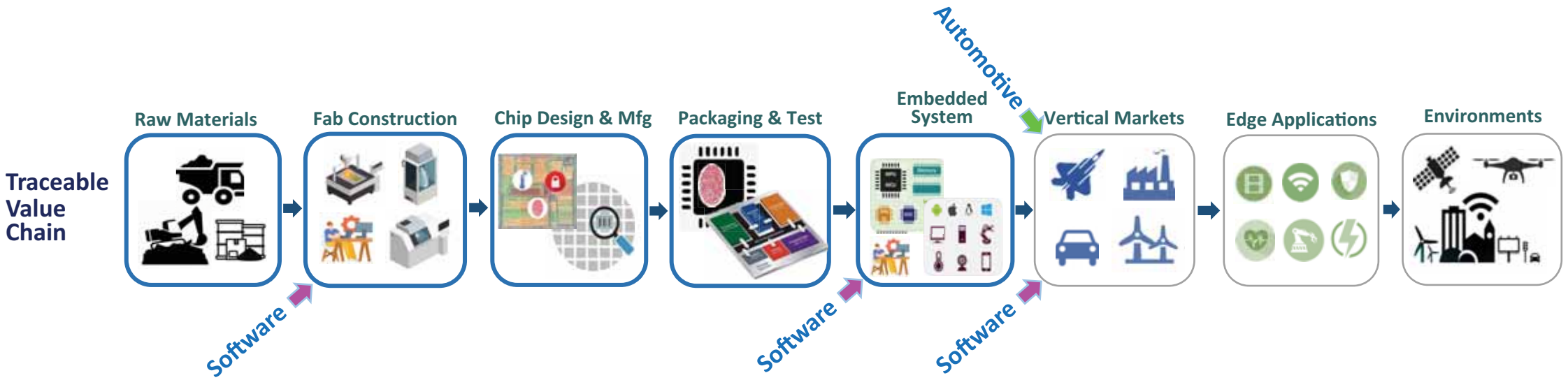
Example of the IETF SCITT in the Automotive Industry

MITRE

Smart Supply Chain Integrity, Transparency & Trust

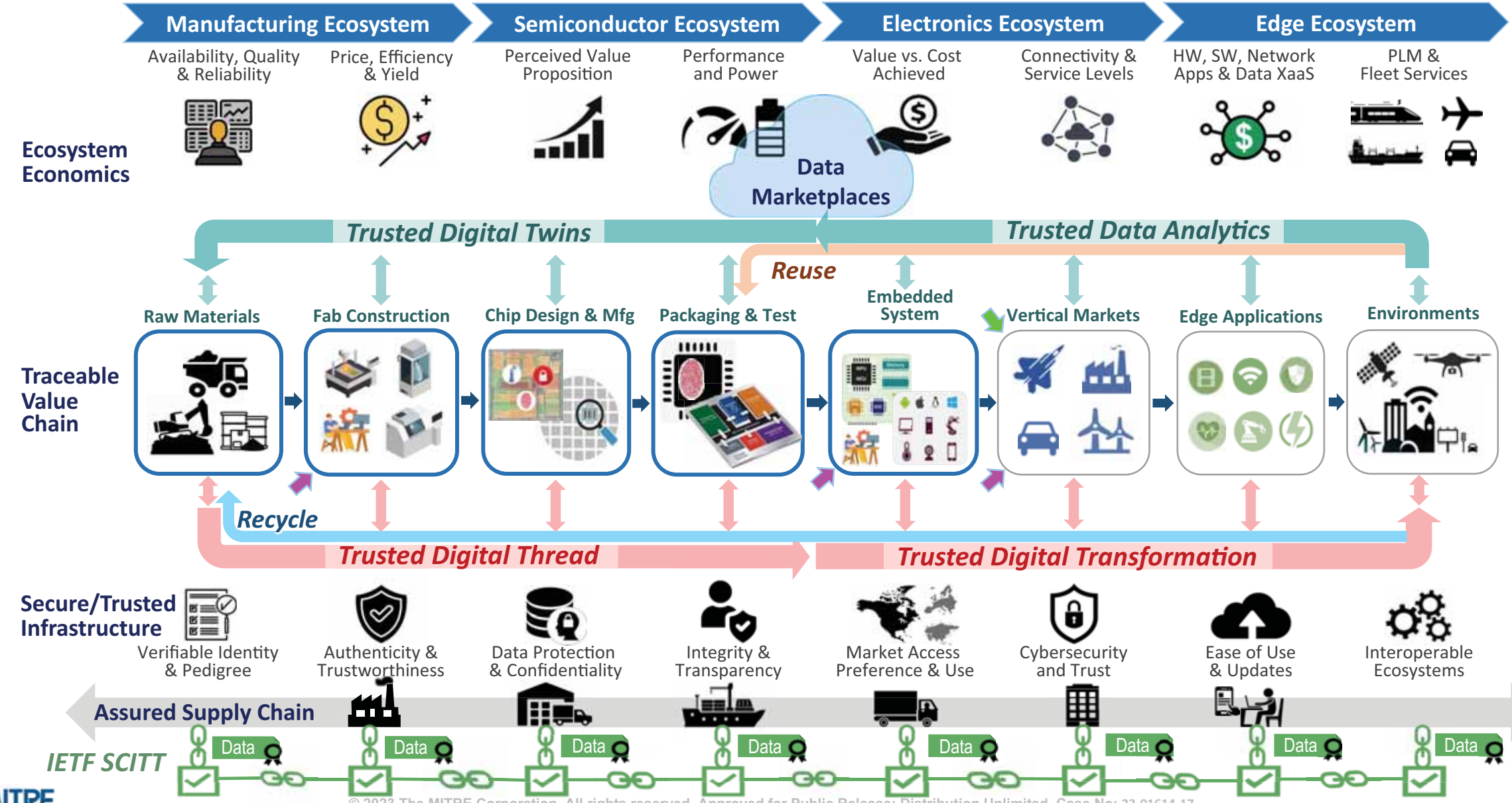
Manufacturing Ecosystem → Semiconductor Ecosystem → Electronics Ecosystem → IoT Ecosystem

Supply Chain Risks (Hazards and Threats)*



* See MITRE's System of Trust repository of potential supply chain risks (SoT.MITRE.ORG)

Smart Supply Chain Integrity, Transparency & Trust



MITRE

Takeaways and Conclusions

- Software exists as a standalone item and as an embedded capability
- Addressing the software supply chain must align and integrate with the other aspects of smart device supply chains.
- Trust, visibility, and integrity needs to be conveyable across all supply chains.
- Assurance is specific to an item and its use in an environmental / business context.
- Automation is critical to gaining and conveying assurance.
- Broadly utilized standards for assurance attestations, BOMs, integrity, vulnerabilities, weaknesses, and risks are needed

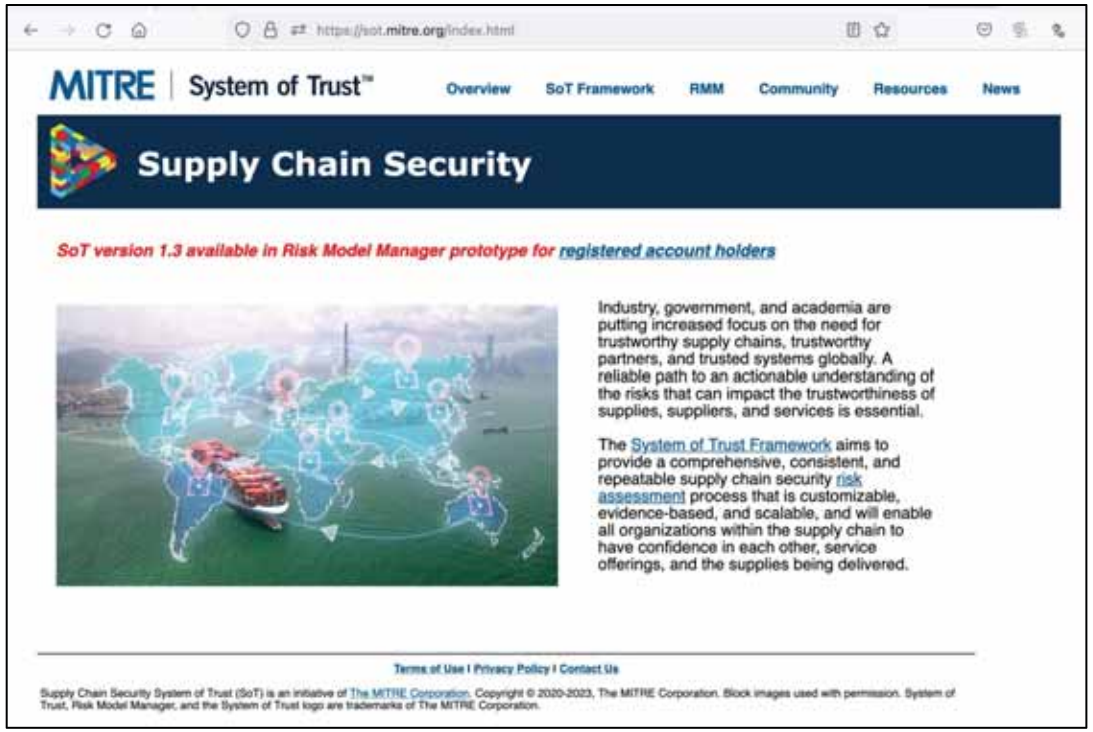
Suggestions for SG17

- Consider making automation guidelines for showing how evolving freely available standardization efforts* across the globe can be used to capture and convey assurance attestations using BOMs and other build claims / statements across supply chains for smart devices and standalone software against appropriately tailored sets of risks for the different environmental / business contexts.

* ISO/IEC 5962 & 5055 (free versions), IETF SCITT, MITRE System of Trust, ITU-T CYBEX (X.1500, X.1520, X.1521, X.1524, X.1525, X.1528), ETSI TR 103 305 (1-4), ETSI TR 103 306, etc.

System of Trust and IETF SCITT

- **MITRE's System of Trust - SoT.MITRE.ORG**
  - **Contact - SOT@mitre.org**
- **SCITT IETF Working Group** - focused on **specification development**. Charter and Meeting schedule outlined by the IETF: https://datatracker.ietf.org/wg/scitt/about/
  - IETF-SCITT Mailing List https://www.ietf.org/mailman/listinfo/scitt
  - IETF 118 (Prague) SCITT Session is planned for Thursday 9 Nov. from 9:30-11:30am



- **SCITT Community** - focused on IETF **specification adoption** https://github.com/ietf-wg-scitt/ including advocacy, outreach, testing, ensuring interoperability of implementations, rapid prototyping, and open source libraries, tooling and examples, like the SCITT API Emulator https://github.com/microsoft/scitt-api-emulator, and View COSE tool https://v.gluecose.org/.
  - The **SCITT Community** is open to the public and new members are invited to join!

MITRE