Supply Chain Security: MITRE’s System of Trust™, SCITT & SBOMs

Robert Martin
Cross Cutting Solutions and Innovation Dept.
Cyber Solutions Innovation Center
MITRE Labs

Presentation to BlackBerry PSEC
30 November 2022
Supply Chain Example – Consumer Clothing

Agriculture (natural fibers)
- Cotton
- Wood

Trims
- PRC
- India
- Southeast Asia

Garments Manufacturer
- PRC
- Bangladesh
- Vietnam
- India
- Turkey

Distributor
- UK
- EU
- USA

Retailer
- UK
- EU
- USA

Consumer

Chemicals (synthetics)
- USA
- Southeast Asia
- Middle East

Yarn
- China
- India
- Southeast Asia
- USA

Textiles
- PRC
- India
- USA
- Turkey
- South Korea

Disposal
Supply Chains

Generic Supply Chain

Materials → Design → Production → Distribution → Customer

Micro-electronics Supply Chain

EDA Tools → 3rd-Party IP Source → Design & Integration → Fabrication & Test → Firmware OTP Values → Provisioning → Deployment

MITRE

© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 22-01488-32
Supply Chains

Generic Supply Chain

- Materials
- Design
- Production
- Distribution
- Customer

Software Supply Chain

- Code
- Commit
- Build
- Test
- Package
- Release
- Deploy
Software is Ubiquitous, Assembled, and Critical

**IT Risk**
- Loss of data or capability
- Loss of safety or reliability
- Loss of property or lives

**Operational Risk**

**Scratch Built Software**
- Majority of products built with no 3rd Party dependencies

**Assembled Software**
- Use of open source and 3rd party libraries, modules, frameworks, and services
- Multi-party software updating/patching

**Traditional Computers**
- Servers: databases
- Desktops: office apps
- Laptops: e-mail
- Tablets: browsers
- Switches: Routers

<table>
<thead>
<tr>
<th>Traditional Computers</th>
<th>Healthcare</th>
<th>Implantable Medical</th>
<th>Smart Munitions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Aeronautics</td>
<td>Smart Manufacturing</td>
<td>Intelligent Vehicles</td>
</tr>
<tr>
<td></td>
<td>Smart Energy</td>
<td>Water Treatment</td>
<td>Intelligent Shipping</td>
</tr>
<tr>
<td></td>
<td>Oil &amp; Gas</td>
<td>Hydro Power</td>
<td>Dam Management</td>
</tr>
<tr>
<td></td>
<td>Microgrids</td>
<td>Smart Cities</td>
<td>Building Management</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Autonomous Systems</td>
</tr>
</tbody>
</table>

© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 22-01488-32
Software Enabled Critical Infrastructure and Mission Capabilities...

Medical

Buildings

Aeronautics

Manufacturing

Vehicles

Energy

Shipping
Whether for Fish, Chips, or Software
Supply Chain Trustworthiness: Intentional

Intentional acts
- Counterfeit products
- Disruption, hijacking, theft, civil unrest,...
- Malicious taint or insertion

Unintentional acts
- Poor quality/tainted goods/shortages/weather disruptions
- Vulnerable software/hardware inserted unintentionally (components/modules w/weaknesses and/or known vulnerabilities)

Result of Supply Chain Attacks:
Systems with adverse behaviors including functional degradation, data exfiltration, espionage, adversarial control and disruption.

Based on SEI/CMU materials
Open Question: What Supply Chain Risks to Manage?
Supply Chain Security (SCS) 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
Risk Categories
- Supplier External Influences
- Supplier Organizational Effectiveness Risks
- Supplier Financial Stability Risks
- Supplier Maliciousness
- Supplier Organizational Security
- Supplier Quality Culture Risks
- Supplier Susceptibility

Supply Risks
- Supply Hygiene Risks
- Supply Counterfeit
- Supply Malicious Taint

Service Risks
- Service Security
- Service Reliability Risks
- Service Quality Risks
- Service Integrity Risks

Trust Aspects
- Ownership and Control Risks
- Foreign Business Relationship Risks
- Adverse Corporate Influences

Basis of Trust
Basis of Trust

Risk Categories
- Environmental, Social, & Governance Risk
- Geographical / Geopolitical Instability
- Structural & Operational Instability

Supplier External Influences
Supplier Organizational Effectiveness Risks
Supplier Financial Stability Risks
Supplier Maliciousness
Supplier Organizational Security
Supplier Quality Culture Risks
Supplier Susceptibility

Supply Hygiene Risks
Supply Counterfeit
Supply Malicious Taint

Service Security
Service Reliability Risks
Service Quality Risks
Service Integrity Risks

Supplier Risks
Supply Risks
Service Risks

Trust Aspects
### Risk Categories
- **Supply External Influences**
- **Supplier Organizational Effectiveness Risks**
- **Supplier Financial Stability Risks**
- **Supplier Maliciousness**
- **Supplier Organizational Security**
- **Supplier Quality Culture Risks**
- **Supplier Susceptibility**

### Supplier Risks

### Supply Risks
- **Supply Hygiene Risks**
- **Supply Counterfeit**
- **Supply Malicious Taint**

### Service Risks
- **Service Security**
- **Service Reliability Risks**
- **Service Quality Risks**
- **Service Integrity Risks**

### Trust Aspects

### Basis of Trust

#### Short-term Financial Health Risks
- Organization has concerning level of liquidity and cash flow
- Organization has concerning ability to pay its debts based on level of debt, assets and equity
- Gross profit margin is of concern
- Organization is not showing a profit

#### Financial Stewardship Risks
- Organization has history of bankruptcy or liens
- Organization has history of being target of lawsuits
- Organization has history of explicit findings/ratings of financial instability due to stewardship issue
- Organization has history of late payments
- Organization has history of SEC (or foreign counterpart) investigations
- Organization lacks currency in public filings

#### Long-term Financial Health Risks
- Company has concerning R&D investment level
- Organization has concerning inventory turnover rate

#### Foreign Financial Obligations
- ...

© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 22-01488-32
## MITRE Supply Chain Security System of Trust Risk Areas*

<table>
<thead>
<tr>
<th>Supplier External Influences</th>
<th>Supplier Financial Stability Risks</th>
<th>Supplier Organizational Effectiveness Risks</th>
<th>Supplier Risks</th>
<th>Supply Chain Risks</th>
<th>Supply Risks</th>
<th>Service Risks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ownership and Control Risks</td>
<td>Financial Stewardship Risks</td>
<td>Environmental, Social, and Governance Risks</td>
<td>Supplier Susceptibility</td>
<td>Supply Risk</td>
<td>Supplier Malicious Taint</td>
<td>Supply Counterfeit</td>
</tr>
<tr>
<td>Foreign Business Relations</td>
<td>Short-term Financial Health Risks</td>
<td>Geographical/Geopolitical Instability</td>
<td>Supplier Culture Risks</td>
<td>Supplier Security Risks</td>
<td>Supply Hygiene Risks</td>
<td>Logistics / Transportation Integrity Risks</td>
</tr>
<tr>
<td>Adverse Corporate Influence</td>
<td>Long-term Financial Health Risks</td>
<td>Structural &amp; Operational Instability</td>
<td>Supplier Maliciousness</td>
<td>Supplier Risk</td>
<td>Supply Malicious Taint</td>
<td>Unsanctioned Manufacturing</td>
</tr>
<tr>
<td>Adverse Market Factors</td>
<td></td>
<td>Susceptible Location</td>
<td>Supplier Organizational Security Risks</td>
<td>Supplier Risk</td>
<td>Supply Counterfeit</td>
<td>Infract Manufacturing</td>
</tr>
<tr>
<td>Adverse Financial Obligation</td>
<td>Technical Susceptibility</td>
<td>Supplier Relations</td>
<td>Supplier Risk</td>
<td>Supplier Risk</td>
<td>Supply Counterfeit</td>
<td>Manufacturing Process Integrity Risks</td>
</tr>
</tbody>
</table>

* Supply Chain Security Top 75 Risk Areas Levels 1-4
** System of Trust Expanding to Pharma, Food, and other types of Products

---

MITRE’s Supply Chain Security System of Trust™️

https://sot.mitre.org/

© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 22-01488-32
Tying together SoT and RMM
Tying together SoT and RMM
System of Trust Pilot 1: Companies of Interest

Supplier and Public Data Profile of the System of Trust Using 5 Risk Categories With 26 Risk Factors
GOAL for use of SoT in Industry and Government…
Supply Chains

Software Supply Chain

Dependencies

Code → Commit → Build → Test → Package → Release → Deploy
Supply-chain Levels for Software Artifacts (SLSA)

SLSA guidelines have 4 levels of incremental and actionable things that software producers can claim to do to protect against specific integrity attacks

https://github.com/slsa-framework/slsa
Supply Chains

Software Supply Chain

- Code compromise source control
- Commit malicious commit
- Build malicious plug-ins
- Build tasks
- Build with build agent/ compiler
- Test tamper with build cache
- Use bad package
- Package compromise package repository
- Release modify release tasks
- Modify build drop prior to release
- Deploy tamper with versioning and update process

Hazards and Threats

malicious 3rd party package or version Dependencies

compromised credentials, hacked email, phishing...
Software Development and Assurance Lifecycle Phases

- Operational Need
- Delivered Capability
- Business or Mission Analysis
- CONOPS Analysis
- Stakeholder Needs & Requirements Definition
- System Requirements Definition
- Attack Surface Analysis
- Architecture Definition
- Design Definition
- Attack Surface Analysis
- System Analysis
- Support Development
- Design
- Product
- Validate Solution
- Continuous Application Across Software Lifecycle
- Transition
- Implementation
- Integration
- Verification
- Operation
- Validation
- Sustainment and Continuous Engineering
- Disposal
- Red Teaming
- Blue Teaming
- Pen Testing
- Dynamic Analysis Tool C
- Fuzz Testing
- Static Analysis Tool B
- Static Analysis Tool A

**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.


© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 22-01488-32
Deployment Example of SCITT in SW Development

- **Policy Gate**
  - Example policy: All commits signed by approved developers
  - Example policy: Source provenance acceptable
  - Example policy: Third-party packages match their BOMs
  - Example policy: Build environment BOM acceptable
  - Example policy: Build output BOM matches published package
  - Example policy: Scan results acceptable
  - Example policy: Release approved
  - Build output BOM matches deployment payload
  - Build configuration acceptable
  - No known unmitigated vulnerabilities

- **Producer**
  - Code
  - Commit
  - Build
  - Test
  - Package

- **Consumer**
  - Release
  - Deploy

- **Signed Evidence**
  - Example evidence: Commit signature proof
  - Example evidence: Build trigger record
  - Example evidence: Build parameters
    - Build environment BOM
    - Build output BOM
  - Example evidence: SAST/DAST scan results
    - Fuzz test results
  - Example evidence: Release approval
  - Example evidence: Release completion

- **Vendor's SCITT Registry**
- **Evidence Entries**
Supply Chains

Micro-electronics Supply Chain

EDA Tools ➔ Materials ➔ Fabrication & Test ➔ Firmware OTP Values ➔ Provisioning ➔ Deployment ➔ 3rd-Party IP Source
Electronics Supply Chain

Attack Functional Characterization

- How can an attack be decomposed into its functional ingredients?
- These ingredients may be how a countermeasure prevents/detects/mitigates the attack.
- Ingredients may be easier to simulate and generate data for
Supply Chains

Micro-electronics Supply Chain

EDA Tools

Materials

Firmware OTP Values

Firmware Updates

Design & Integration

Fabrication & Test

Provisioning

Deployment

Hazards and Threats
Deployment Example of SCITT in Chip Development

Policy Gate →

Producer → EDA Tools → Materials → Firmware, Bitstream and OTP Values → Firmware Updates → Consumer

3rd Party IP Source → Design & Integration → Fabrication & Test → Provisioning → Deployment

Policy Entries → Vendor's SCITT Registry

Signed Evidence → Evidence Entries

Example policy:
- All design and integrity checks pass
- Source design artifacts are correct and unaltered
- Licenses for IP in order
- Substrate tests check
- Trace circuitry checks
- Product conforms to design
- Chip passes acceptance tests
- Chip electrically acceptable
- Release approved
- Build output BOM matches deployment payload
- Build configuration acceptable
- No known unmitigated vulnerabilities

Example evidence:
- IP blocks used are signed
- IP blocks are licensed correctly
- EDA tools analysis is clean
- Mask is integrity protected
- Mask is sent through private channel
- Receipt by FAB verified
- Silicon fab quality check passed
- Production conforms to design
- Integrity and performance checks pass
- Chip packaged correctly
- Chip tested for basic conformance to design
- Firmware image applied correctly
- Release completion
- Reports on product updates and warranty claims
- Operational logs
- Disposition / Disposal / Recycling Logs
Supply Chains

Seafood Supply Chain

Harvesting

- Hold heats up

Landing & Processing

- Fish in hold too long to be labelled as fresh fish
- Packaging incorrectly assembled
- No food quality pallets available

Distribution

- Incorrect delivery order barcodes generated
- Wrong barcodes applied
- Fish heat up

Retail & Commercial Food Services

- No sales
- Partial sales

Consumers

- Customer gets sick
- Incorrect goods provided to customer

Hazards and Threats
Deployment Example of SCITT in Harvesting Fish

Producer

Harvesting

Landing & Processing

Distribution

Retail & Commercial Food Services

Consumer

Policy Gate →

Example policy:
• Ship hold temperature remains below safe limits

Example policy:
• Cargo stored at safe temperature
• Cargo meets freshness limits

Example policy:
• Fish packaged for shipment and labeled appropriately
• Containers correctly maintain temperature

Example policy:
• Barcodes of delivered goods match destination
• Temperature maintained

Example policy:
• Fish sold within freshness date
• Fish maintained temperature throughout movement

Signed Evidence →

Example evidence:
• Temperature of fish storage hold

Example evidence:
• Harvest in storage for less than maximum days allowed for fresh fish

Example evidence:
• Lean inspections
• Appropriate labels produced
• Appropriate packaging assembled
• Appropriate pallets used to pack for delivery

Example evidence:
• Delivery barcodes issued and applied
• Shipping manifests delivered to receiving locations

Example evidence:
• Fish sold to consumer

Example evidence:
• Consumer complaints
• Consumer feedback
• Store feedback
• Distributor feedback

Vendor's SCITT Registry

Policy Entries

Evidence Entries

© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 22-01488-32
SCITT Concepts

Claim → Registration Policy → Notary → Transparent Registry → Receipt
**SCITT Definitions & Terms**

**Claim:** Identifiable, non-repudiable statement about an **Artifact** made by an **Issuer**.

**Registration Policy:** Pre-condition for registering a claim.
This involves verifying the claim issuer, and may depend on other claim attributes and previously-registered claims.

**Notary:** **Transparency service** that receives claims; checks they pass its registration policy; registers them; and returns their receipts.

**Registry:** Verifiable data structure providing a consistent append-only log for all registered claims.

**Receipt:** Offline, universally-verifiable proof that a claim is recorded in the registry.
Claims and receipts do not expire, but newly registered claims may subsume older claims.

**Verifier:** Entity that receives claims + receipts and verifies them before using their contents

**Auditor:** Entity that checks the correctness and consistency if all claims in the registry.

---

Deployment Example of SCITT in the Marketplace
Deployment Example of SCITT in the Marketplace
Deployment Example of SCITT in the Marketplace

One of the SCITT Registries

Producer

Endorser

Artifact 1 (b)
Claim & Evidence 1 (c)

Consumer

Consumer Agent
Policy Manager
Deployment Example of SCITT in the Marketplace
Deployment Example of SCITT in the Marketplace
SCITT Architecture Model

![SCITT Architecture Diagram]
SCITT Standard Components

Issuer Identification (re-using DID)

Formats for Signed Claims (using CBOR and COSE)

Claim Endorsements

Registration Policies

Algorithms for Transparent Registry (Merkle trees)

Formats for Receipts

Auditing

Goal of SCITT is to simplify and standardize these interactions
SCITT Roadmap

Industry Standards

- Internet Engineering Task Force (IETF) Working Group
  - SCITT Charter [https://datatracker.ietf.org/wg/scitt/about/](https://datatracker.ietf.org/wg/scitt/about/)
  - Current tasks: gathering use cases and working draft documents
    - IETF-SCITT GitHub Repository [https://github.com/ietf-scitt/](https://github.com/ietf-scitt/)
    - IETF-SCITT Use Cases [https://github.com/ietf-scitt/use-cases/](https://github.com/ietf-scitt/use-cases/)
    - SCITT architecture draft:
      - [An Architecture for Trustworthy and Transparent Digital Supply Chains](#)
    - SCITT countersigning draft:
      - [Countersigning COSE Envelopes in Transparency Services](#)

- IETF 116 (Yokohama) SCITT Session is planned for Thursday 30 March from 9:30-11:30am
Software related policy

EO 14028 part 4

May 12, 2021

Executive Order on Improving the Nation’s Cybersecurity

By the authority vested in me as President of the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, private sector, and ultimately the American people’s security and privacy. The Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to those actors and actions. The Federal Government must also carefully examine what occurred during any major cyber incident and apply lessons learned. That cybersecurity requires more than government action. Protecting our Nation from malicious cyber actors requires the Federal Government partner with the private sector. The private sector must

https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/


DoC / NTIA Minimal Elements of an SBOM

NIST SP 800-218 SSDF

NIST Special Publication 800-218

Secure Software Development Framework (SSDF) Version 1.1:
Recommendations for Mitigating the Risk of Software Vulnerabilities

Munirah Isaopua
Karim Saffari
Donna Dickson

The United States Department of Commerce

July 12, 2021

This publication is available free of charge from:
https://doi.org/10.6028/NIST-SP.800-218


OMB memo M-22-18

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shalanda D. Young
Director

SUBJECT: Enhancing the Security of the Software Supply Chain Through Secure Software Development Practices

The Federal Government relies on information and communications technology (ICT) products and services to carry out its critical functions. The global supply chain for these technologies faces information threat from state and criminal actors seeking to steal sensitive information and intellectual property, compromise the integrity of Government systems, and conduct other acts that impact the United States Government’s ability to safely and reliably provide services to the public.

Executive Order 14028, Improving the Nation’s Cybersecurity (May 12, 2021), focuses on the security and integrity of the software supply chain and emphasizes the importance of secure software development practices. The EO directs the National Institute of Standards and Technology (NIST) to issue guidance “identifying practices that enhance the security of the software supply chain.” The Secure Software Development Framework (SSDF), SP 800-218, and the NIST Software Supply Chain Security Guidance (these two documents, taken together, are hereafter referred to as “NIST Guidance”) include a set of practices that create the foundation for developing secure software. The EO further directs the Office of Management and Budget (OMB) to require agencies to comply with such guidelines. This memorandum requires agencies to comply with the NIST Guidance and any subsequent updates.


© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 22-01488-32
SBOM Definition

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

Minimum Elements

<table>
<thead>
<tr>
<th>Data Fields</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Automation Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Practices and Processes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Define the operations of SBOM requests, generation and use including: Frequency, Depth, Known Unknowns, Distribution and Delivery, Access Control, and Accommodation of Mistakes.</td>
</tr>
</tbody>
</table>


SPDX
CycloneDX
SWID


HBOMs – ICT SCRM Task Force
Supported by both formats


SBOM Communications Channels and Use Cases

**Acquisitions**
(Pre & Post Acquisition)

**Acquisition Software Assurance Assessment**
- Validate software meets requirements for acquisition
- Flag issues for remediation before deployment

**Software Bill of Materials (SBOM) Elements**
SBOM Communications Channels and Use Cases

- Inventory SBOM for each version of software
- Identify software exposed to new vulnerabilities
- Quickly identify where portfolio is exposed to emerging threats
SBOM Communications Channels and Use Cases

- Define reporting and scanning requirements
- Define and maintain blocklist/allowlist of SBOM components
- Define risk thresholds for emerging threats (e.g. new CVEs for existing software)
- Define mitigation and remediation protocol
SBOM Communications Channels and Use Cases

Vulnerability Management
(Patching, Updates & Versioning)

Software Bill of Materials (SBOM) Elements

- Verify upgrade / patch/version meets blacklist / allowlist component requirements
- Verify software and SBOM components free of policy-violating vulnerabilities
SBOM Communications Channels and Use Cases

Software Bill of Materials (SBOM) Elements

- Use SBOM to quickly identify emerging threat exposure
- Target mitigation for compensating controls
- Target patching across software portfolio
SBOM Communications Channels and Use Cases

- Map emerging Open Source threats embedded in software supply-chain
SBOM Communications Channels and Use Cases

- Identify disallowed SBOM components
- Drive remediations requirements to supplier
- Identify vulnerabilities and other OSS policy violations
- Verify software standards
- Applies to patches/updates/upgrades
SBOM Communications Channels and Use Cases

- Monitor that software complies with standards across software life cycle
- Pre-installation scan of patches / updates / upgrades
SBOM Communications Channels and Use Cases

**Contract requirements:**
- 3rd party scanning chosen by agency required
- Vendor provides software for SBOM Validation
- On-going scanning req’t across software life-cycle

**Legal (Licensing)**

**Software Bill of Materials (SBOM) Elements**
SBOM Communications Channels and Use Cases

Agency to Supplier
- Assessment Request
- Security Policy/Risk threshold
- Request remediation from / to Supplier
- Supplier to Agency
- Request acceptance
- Published results
- Results annotation
SBOM Communications Channels and Use Cases

**Agency to Supplier**
- Assessment Request
- Security Policy/Risk threshold
- Request remediation from / to Supplier
- Supplier to Agency
- Request acceptance
- Published results
- Results annotation

**Contract requirements:**
- 3rd party scanning chosen by agency required
- Vendor provides software for SBOM Validation
- On-going scanning req’t across software life-cycle
- Monitor that software complies with standards across software life cycle
- Pre-installation scan of patches / updates / upgrades
- Identify disallowed SBOM components
- Drive remediations requirements to supplier
- Identify vulnerabilities and other OSS policy violations
- Verify software standards
- Applies to patches/updates/upgrades
- Map emerging Open Source threats embedded in software supply-chain

**Software Bill of Materials (SBOM) Elements**

**Acquisitions (Pre & Post Acquisition)**
- Validate software meets requirements for acquisition
- Flag issues for remediation before deployment

**Asset Management (Post Acquisition)**
- Inventory SBOM for each version of software
- Identify software exposed to new vulnerabilities
- Quickly identify where portfolio is exposed to emerging threats

**Policy (SBOM Standard & Risk Threshold)**
- Define reporting and scanning requirements
- Define and maintain blocklist/allowlist of SBOM components
- Define risk thresholds for emerging threats (e.g. new CVEs for existing software)
- Define mitigation and remediation protocol

**Vulnerability Management (Patching, Updates & Versioning)**
- Verify upgrade / patch/version meets blocklist / allowlist component requirements
- Verify software and SBOM components free of policy-violating vulnerabilities

**Incident Response**
- Use SBOM to quickly identify emerging threat exposure
- Target mitigation for compensating controls
- Target patching across software portfolio

**Deployment (Authority to Operate)**
- Threat Intelligence (OSS Package)
- Continuous Monitoring (Post Acquisition, Requirements & Remediation)

**Legal (Licensing)**

**Communications (Vendor Interactions)**
Three MITRE and one Atlantic Council SBOM papers


Supply Chains – As multi-Stakeholder Network

https://www.iiconsortium.org/pdf/Trustworthiness_FrameworkFOUNDATIONS.pdf

© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 22-01488-32
Examples of System of Trust Engagements

- DHS S&T Program Office
- American Bar Association (ABA) Technology Meeting
- Industry Technology & Innovation Roundtable
- Open Group July Member Meeting Plenary
- ABA IoT National Institutes Panel
- DoD/DoE NNSA Software Assurance Community of Practice
- DHS S&T FVEYS Supply Chain Workshop
- EOP/OMB — Mana Root (Dep Fed CIO at OMB)/ Camilo Sandoval (Fed CISO)
- EOP/OMB w/ Wesley Field / Matthew Blum / Jeremy McCray — OFPP Team
- Raytheon Technologies Product Cybersecurity Tech Exchange
- Senate Homeland Security and Governmental Affairs Committee staff
- IIC Winter 2020 Quarterly Member Meeting
- House Homeland Security Committee staff
- ABA SciTech Lawyer article — Winter 2021 issue
- GAO Supply Chain Report Authoring Team
- ATIS 5G/SC Working Group
- House Armed Services Committee staff
- Senate Armed Services Committee staff
- House Oversight Committee staff
- Chris DeRusha (Fed CISO)
- Soraya Correa (DHS CPO)
- DHS C5NG Supply Chain Subgroup
- USEA Energy Technology and Governance Program UCSI Working Group
- ABA IoT National Institute
- IIC Summer Meeting
- Manufacturing Industry Leadership Council meeting
- Global Industry Organizations’ Smart Manufacturing Workshop
- SAE G-32 Hardware WG meeting
- New England Council event
- NSTAC Software Assurance Sub-Committee
- Aerospace Industries Association
- TIA / OiFEST Forum Supply Chain Security 9001 Webinar
- Staff of Rep. Elissa Slotkin

Executive Acquisition
Congressional Committees

- HASC critical defense supply chain TF report Staff
- ADM Mauger US Coast Guard Assistant Commandant for Prevention Policy (CG-SP)
- Navy Research, Development & Acquisition (ASN/R&D&A)
- House Committee on Oversight and Reform
- Q3 IIC Information Day - Fuel Your Digital Transformation Journey
- CISA NRMAC Supply Chain Trustworthiness Framework IPT
- CISA Standards Area Lead for C-SCRM
- MDA Ground Missile Defense PM
- DoE/CEER Cybersecurity Senior Advisor
- House Permanent Select Committee on Intelligence
- Electric Power Research Institute (EPRI)
- Common Attack Pattern Enumeration (CAPEC) Workshop
- HHS ASPR RISC 2.0 Leadership Team
- DoE SCRM Team
- IIC March 2022 Event
- SW Supply Chain Integrity and SoT to EoIP Team
- CMS CIO
- ELISA Workshop
- CISQ Webinar
- Software Supply Chain Security Webinar
- System of Trust with VA SCRM Team
- SW Supply Chain Integrity and SoT to RKST Team
- SW Supply Chain Integrity and SoT to Dell Team
- American Bar Association (ABA) Technology Meeting
- RSA Conference 2022
- Open Group July Member Meeting Plenary
- Hacks In Taiwan Conference 2022
- Hot Topics in Supply Chain Security 2022 Summit
- NDIA Microelectronics Trust and Assurance Workshop
- ABA IoT National Institute 2022
- CISQ Resilience Summit
- Third Party Risk Management Symposium in Sao Paulo Brazil
- Cyber Physical Systems Symposium in Tokyo Japan
- others...

© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 22-01488-32
System of Trust Plans with Sponsors and Industry

Assessment Capabilities for Sponsors, Industry and Academia

Training Sponsors & Industry on the SoT methodology, content, and platform

Standards and best practices oriented around SoT

Evolving SoT BoK with Domain SMEs to enhance Risk Factors

Mapping SoT to Industry and Government standards and assessment mechanisms

Active Feedback with communities on enhancements to SoT

No-Cost* Licensing RMM tool & SoT content to Industry for integration in their own assessment practices and offerings

*No-Cost means the tool is provided at no charge to the Industry for the integration of SoT content.
Publications to date...

https://www.cutter.com/offer/supply-chain-security-system-trust


https://www.mitre.org/publications/technical-papers/supply-chain-security-it’s-everyone’s-business
Industry, government, and academia are putting increased focus on the need for trustworthy supply chains, trustworthy partners, and trusted systems globally. A reliable path to an actionable understanding of the risks that can impact the trustworthiness of supplies, suppliers, and services is essential.

The System of Trust Framework aims to provide a comprehensive, consistent, and repeatable supply chain security risk assessment process that is customizable, evidence-based, and scalable, and will enable all organizations within the supply chain to have confidence in each other, service offerings, and the supplies being delivered.
Growing Engagement about System of Trust

<table>
<thead>
<tr>
<th>Organization</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Company 1</td>
<td>Microelectronics SMEs</td>
</tr>
<tr>
<td>Company 2</td>
<td>Supply Chain Illumination SMEs</td>
</tr>
<tr>
<td>Company 3</td>
<td>Critical Infrastructure SMEs</td>
</tr>
<tr>
<td>Company 4</td>
<td>Supply Chain Illumination SMEs</td>
</tr>
<tr>
<td>Company 5</td>
<td>Organization with Supply Chains</td>
</tr>
<tr>
<td>Company 6</td>
<td>Organization with Supply Chains</td>
</tr>
<tr>
<td>Company 7</td>
<td>Cybersecurity Illumination SMEs</td>
</tr>
<tr>
<td>Company 8</td>
<td>Cybersecurity Illumination SMEs</td>
</tr>
<tr>
<td>Company 9</td>
<td>Supply Chain Illumination SMEs</td>
</tr>
<tr>
<td>Company 10</td>
<td>Organization with Supply Chains</td>
</tr>
<tr>
<td>Company 11</td>
<td>Community Engagement SMEs</td>
</tr>
<tr>
<td>Company 12</td>
<td>Organization with Supply Chains</td>
</tr>
<tr>
<td>Company 13</td>
<td>Organization with Supply Chains</td>
</tr>
<tr>
<td>Company 14</td>
<td>Organization with Supply Chains</td>
</tr>
<tr>
<td>Company 15</td>
<td>Supply Chain Illumination SMEs</td>
</tr>
<tr>
<td>Company 16</td>
<td>Organization with Supply Chains</td>
</tr>
<tr>
<td>Company 17</td>
<td>Retail Banking SMEs</td>
</tr>
<tr>
<td>Company 18</td>
<td>Third Party Risk Management SMEs</td>
</tr>
<tr>
<td>Company 19 (plus 20 more)</td>
<td>Sustainability SMEs</td>
</tr>
</tbody>
</table>