Roles and Benefits for SBOM Across the Supply Chain

NTIA Multistakeholder Process on Software Component Transparency
Use Cases and State of Practice Working Group

Introduction

Software is everywhere. Like steel and concrete, software increasingly plays a foundational role in a modern, connected society and like those other building materials, how and with what ingredients the building materials are created often matters. Software permeates banking, healthcare, utilities, emergency services, national defense, government systems, and the like. The software includes operating systems, firmware, and embedded systems within our gadgets, devices, IoT, and other machines. And just like these physical goods, the software has a supply chain that may need to be understood and managed by an organization dependent on that software.

Most software includes other software. Software changes and evolves over time due to optimization, new features, security fixes, and so forth. As a result, software producers throughout the supply chain have to continually evaluate how changes might impact their software. This includes changes to 3rd-party components used to compose software. How can organizations make confident, informed decisions? How can they manage the complexity of their software supply chain in a sustainable manner? In a complex supply chain, roles can blur. For simplicity, we will initially describe the software supply chain from three perspectives:

- I *produce* software - the person/organization that creates a software component or software for use by others [write/create/assemble/package]
- I *choose* software - the person/organization that decides the software/products/suppliers for use [purchase/acquire/source/select/approve]
- I *operate* software - the person/organization that operates the software component [uses/monitor/maintain/defend/respond]

This list is not a comprehensive list of perspective, there are other roles such as auditors, insurers and such who will also benefit from an SBOM as it matures and the various use cases evolve. These three perspectives are summarized in the following table:

	Perspective on Software		
Benefit	**Produce**	**Choose**	**Operate**
Cost	Less unplanned, unscheduled work	A more accurate total cost of ownership	More efficient administration
Security Risk	Avoid known vulnerabilities	Easier due diligence	Faster identification and resolution. Know if and where specific software is affected
License Risk	Quantify and manage licenses and associated risk	Easier due diligence	More efficient, accurate response to license claims
Compliance Risk	Easier risk evaluation. Identify compliance requirements earlier in lifecycle	More accurate due diligence, catch issues earlier in lifecycle	Streamlined process
High Assurance (See Appendix II)	Make assertions about artifacts, sources, and processes used.	Making informed, attack-resistant choices about components.	Validate claims under changing and adversarial conditions.

Table 1: Software Bill of Materials - Perspectives and Benefits

The Software Supply Chain

Even before software was widespread, organizations thought about multi-stage production processes through the lens of the *supply chain*: each stage of production takes inputs from a previous stage and adds their own skills and contributions to produce outputs that a subsequent stage can use. At one end are the most basic components, such as raw materials, and at the other end are the final users or consumers of the product. Each link in the well-functioning supply chain provides an opportunity to ask crucial questions, such as "Does this input meet my quality standards?" and "Am I using the correct input, or should I use something else?"

It's useful to think of modern-day software development as a supply chain:

- Software developers write code that fulfills a need, then make it available freely or commercially.
- Other developers with similar needs find that code and include it in their own software.
- At some point, a product manufacturer assembles software components into a product.
- End users acquire and operate the finished product.

The supply chain is a simple model of how products are made, but it doesn't answer every possible question. What happens when something goes wrong with a link in the chain?

In the world of physical goods, "upstream" parts might be recalled or upgraded, and the relationships in the supply chain might be strong enough to make sure that any necessary changes are made "downstream."

In the world of software, the links between dependencies are weaker. Sometimes, there is no direct commercial relationship between the links. And unlike most physical parts, software components change constantly. Every participant in the software supply chain is continually weighing choices and grappling with changes introduced by the release of new software versions, security vulnerabilities, and shifting requirements. Because of the complex web of dependencies in software supply chains, any change can have far-reaching effects.

About this document: Goals and Methodology

This document was drafted by the Use Cases Working Group as part of NTIA's multistakeholder process on software component transparency.[1] The group was initially driven by several observations. First, participants noted that SBOMs (and things like them) were already in use today, and thus the existing use cases should be documented and captured. Second,

[1] More information about the multistakeholder process, including all the interim drafts, is available at https://www.ntia.doc.gov/SoftwareTransparency. The initial deliverables of this process, including this document, are available at https://www.ntia.gov/sbom.

participants embraced the idea that lack of transparency was a supply chain problem, and any transparency solution should address the broader software supply chain rather than any single subset or sector. Third, stakeholders argued that since the benefits of transparency accrue through different mechanisms across the supply chain, these benefits should be carefully mapped out. A key aspect of this work was to understand how the efforts of the broader NTIA initiative could impact the software ecosystem and increase awareness and adoption for the growing community of those interested in SBOM practices.

The group set out with two goals: to capture the SBOM use cases today to find out what works and what needs to be improved and to understand how existing software practices could be improved by wider adoption of SBOMs. Participants wanted to avoid further reinventing the wheel at each organization facing their own software supply chain challenges. As noted in Appendix I, this work is not happening in a vacuum. There is a growing awareness of the importance of SBOMs, and many efforts to address it.

Much of this work was inspired by existing industrial and supply chain work.[2] We have adapted the framing of earlier work to better match the structure of today's software industry and make the lessons learned more accessible. The group held weekly conference calls to extract knowledge and debate these use cases. The expertise of working group members was supplemented by a series of interviews with different actors in the supply chain. Each interview lasted at least half an hour and consisted of detailed questions to understand the interviewees' ideas of the risks, costs, and potential value of software transparency. The group decided to focus on the points of view of three perspectives (as discussed above) and capture the current or potential benefits that greater software transparency can provide.

This document is supplemented by two appendices. Appendix I contains references to other initiatives that explicitly or implicitly acknowledge the value and importance of transparency in the supply chain. Appendix II contains a discussion of the value from assurance attributes around SBOMs that may be necessary for certain applications. These higher assurance points will be addressed in the future work of the NTIA process.

Perspective: Produce Software

Code reuse is an integral part of modern software. In addition to writing their own code, producers of software routinely integrate third-party code and components into their software. Organizations that make software continually weigh whether to build components from scratch

[2] See "Toyota Supply Chain Management: A Strategic Approach to Toyota's Renowned System" by Ananth V. Iyer, Sridhar Seshadri, and Roy Vasher – a work about Edwards Deming's Supply Chain Management
https://books.google.com/books/about/Toyota_Supply_Chain_Management_A_Strateg.html?id=JY5wqdelrg8C

or import components from elsewhere. To keep projects moving at high velocity, this decision making is often diffused among teams and individual developers. Yet consideration of components or ingredients in any product is a key piece to producing a high-quality product.

For many organizations, review, and vetting of open-source software, they choose to include in their products and services began because of restrictive open-source licenses that put limitations on distribution. However, it was quickly recognized that open source software caused security concerns as well. A bill of materials is integral to understanding the supply chain of any product, and in the software space, it is hard to understand anything about the supply chain risk without visibility into these underlying components.

A Software Bill of Materials (SBOM) can help a software supplier produce their software in the following ways:

- reduce unplanned, unscheduled work
- reduce code bloat.
- adequately understand dependencies within broader complex projects
- know and comply with the license obligations
- monitor components for vulnerabilities
- end-of-life (EOL)
- make code easier to review
- a blacklist of banned components
- provide an SBOM to a customer

Reduce unplanned, unscheduled work

An SBOM can **reduce unplanned, unscheduled work** by offering better visibility into the codebase, which in turn leads to better prioritization and quicker delivery for code updates. For example, when a new vulnerability emerges, without an SBOM, a software engineering team would have to review all their software to determine if any of it has a problem. Using an SBOM, any software that might contain that vulnerability is easily identified. The organization can both increase the priority of required bug fixes and can save time by not having to further review identified components and focus more on reviewing the rest of the software.

Reduce code bloat

An organization that tracks components can more easily **reduce code bloat.** Open source components, in particular are often available in dozens of slightly different versions that perform the same functions, and each version potentially has different and unique defects. SBOMs make it easier for an organization to standardize on a common set of components, so any vulnerability will need to be corrected only on a single component.

Adequately understand dependencies within broader complex projects

More broadly, making it easier for developers to **adequately understand dependencies within broader, complex projects** can facilitate more responsibility and better quality management. A more systematic approach to code reuse can allow greater confidence in the overall process and therefore product. An organization can better track needed experience/expertise for particular teams or products, make sure that potential future maintenance is supportable, and avoid surprises when downstream customers evaluate the software.

Know and comply with the license obligations

It enables an organization to **know and comply with the license obligations** of the components used. A system that makes licensing policies easy to use can help automate license compliance.

Monitor components for vulnerabilities

An SBOM-equipped producer can more easily **monitor components for vulnerabilities** so the team can more proactively evaluate and remediate risks. When a new security risk is discovered by security researchers, identifying whether or not a particular product is potentially vulnerable can be a drawn-out process. An easily accessible list of components can make this process much more efficient. Better awareness of components can also shorten the window to reassure customers, improving customer trust.

End-of-life (EOL)

Sometimes, software components reach their **end-of-life (EOL)** and are no longer supported by that upstream supplier, or the supplier disappears entirely. A responsible producer should actively monitor for this, and plan for contingencies before they arrive. An SBOM enables an organization to be proactive with their supply chain to identify and implement alternative solutions.

Make code easier to review

Tracking components and subcomponents can **make code easier to review** and understand for developers, simplifying builds and reducing obstacles to getting code into production. Much of the initial security testing for avoidable harm can happen at early stages and in-context, as the code is written/assembled, weeks or months earlier than the alternative. Furthermore, this tracking enables situational awareness when an underlying dependency changes. It can also provide a better understanding of the work and time needed to make a change to the codebase.

A blacklist of banned components

Tracking component usage can support strategies like **a blacklist of banned components** or a whitelist of preferred components **-** or both. Blacklists allow companies to avoid components with known issues, orphaned projects, or that have had a history of having many issues whether they be security, performance or reliability issues. Whitelists, while not as common, allow companies to use trusted third party components and invest in their use, or have a list of preferred providers. SBOMs can foster a feedback loop to better develop more informed approved lists based on operational metrics of suppliers.

Provide an SBOM to a customer

An organization can **provide an SBOM to a customer** or downstream partners to help assure them that the company is providing a high-quality product that meets customers' legal and security needs (see below for how an SBOM can help those who choose and maintain software). Being proactive can offer a competitive advantage as SBOM adoption increases, and may ultimately become a common market expectation or requirement. An up-to-date SBOM can also reassure downstream consumers about the current security status of a product in their possession.

Perspective: Choose Software

Choosing software includes the selection and acquisition of software products. These processes differ from one organization to another, but while there are many ways of choosing software, there are a few well-known steps common to all of them.

Almost any choice of software is a long-lasting commitment, and it is therefore very important that the decision to acquire one software product or component vs. another is made with forethought and planning. This acquisition process can be formal or informal and may include steps such as reviewing requirements, market surveys, evaluating suppliers and products, and the purchasing and receiving to the actual acquisition of the software. It is also likely in a typical organization that several functional teams could be involved, including end users, finance, legal, and technical support.

Consumers of software without an SBOM know there are probably open-source components inside the code that are not exposed by the software supplier. Those ingredients could include unsupported (“orphaned”) libraries or components with known vulnerabilities (See Appendix II below). Malicious suppliers could hide malware inside components that performed useful functions.

An SBOM can help an organization choose their software in the following ways:

- identify potentially vulnerable components
- a more targeted security analysis
- verify the sourcing
- compliance with policies
- aware of end-of-life components
- verify some claims
- understand the software’s integration
- pre-purchase and pre-installation planning
- market signal

Identify potentially vulnerable components

Visibility into underlying components can help **identify potentially vulnerable components**. Prior to purchase, an organization can conduct the basic risk analysis to understand what they are about to install on their systems.

A more targeted security analysis

Organizations with a more mature risk process can engage in **a more targeted security analysis** process by deciding what code components might raise red flags (e.g., a cryptographic library that offers substandard protection) and which components might have already been vetted by a trusted source.

Verify the sourcing

If the SBOM includes signature hashes of the components, an organization can **verify the sourcing** of third-party components to limit the risk that counterfeit or backdoored components slipped into the supply chain of the supplier. (While an SBOM may not directly prevent a determined adversary from interfering with the legitimate source, it can greatly simplify remediation once the attack is detected--see above.) An SBOM's integrity and authenticity is discussed in more detail in the complementary documents "Framing Software Component Transparency" and the "Survey of Existing SBOM Formats and Standards."[3]

Compliance with policies

Organizations may face regulations or other rules around supply chain sources, and an SBOM can enable **compliance with policies** around what must or must not be used in their organization.

Aware of end-of-life components

An organization can be made **aware of end-of-life components** for which future support will not be available. While these components may not be a risk when the software is first acquired, any problem found later in the component will most likely not be fixed.

Verify some claims

The acquirer will be better able to **verify some claims** by the supplier about the codebase and its quality. While knowing which components and versions will not answer every question about the quality and security of software, it can offer some insight into the supplier's vigilance.

[3] These documents are available at https://www.ntia.gov/SBOM.

Understand the software's integration

An organization can better **understand the software's integration** into existing asset and vulnerability management systems, lowering the overall cost of ownership and minimizing the likelihood of risks emerging from poor integration.

Pre-purchase and pre-installation planning

An organization can engage in **pre-purchase and pre-installation planning** for potentially vulnerable or out of date software that it still intends to purchase. Purchase decisions are made for many reasons, and the benefits of purchase and use may outweigh the security risks. In this case, the security team can start to make decisions to treat more at-risk systems differently, including designing segmented networks or white-listed access systems and preparing check-lists for the operational team that will be installing and maintaining the system.

Market signal

Finally, an SBOM provides a **market signal** that a supplier is thinking about possible risks from its included components, indicating the supplier is practicing good software development hygiene and observes some best practices. This can have the most marked impact on the suppliers by rewarding those who invest in security and quality processes.

Choosing software means choosing a supplier, and any choice of a supplier also means inheriting all of its suppliers as a consequence. SBOMs ensure such transparency is possible so the buyer can make a more informed choice.

Perspective: Operate Software

Once any software package or component is selected and acquired, it must be installed, configured, maintained, and administered. We group these responsibilities under the category of “operations.” They vary for different organizations and could cover a range of potential roles, ranging from the administrator to the Network Operations Center (NOC) or Security Operations Center (SOC) to an executive in charge of risk or compliance such as Chief Information Security Officer (CISO). These roles may also apply for non-IT packages such as embedded software in an industrial or Operational Technology (OT) setting.

An SBOM can help an organization configure, maintain, and administer its software in the following ways:

- Organization can quickly evaluate whether it is using the component
- Drive independent mitigations
- Make more informed risk-based decisions
- Alerts about potential end-of-life
- Better support compliance and reporting requirements
- Reduce costs through a more streamlined and efficient administration

Organization can quickly evaluate whether it is using the component

A list of components allows for the discovery and association of new vulnerabilities as it applies to software in their current environment. An SBOM allows an organization to understand what components are active on its systems and networks. When any new flaw in a particular component is discovered, the **organization can quickly evaluate whether it is using the component**, and therefore whether it is at risk.

Drive independent mitigations

Awareness of underlying potentially risky components can **drive independent mitigations** while an organization waits for their supplier to assess the actual risk and provide software updates as needed. Some organizations may decide to take defensive action on their own to minimize risks from known vulnerable software. Examples of possible actions include compensating procedural controls, technical isolation of an affected system, or increased scrutiny of system activity. If a defective software component is not actively supported by the supplier, or the supplier doesn't exist anymore, these measures may be the only possible mitigation.

Make more informed risk-based decisions

More broadly, an SBOM allows an operator to **make more informed risk-based decisions** about what is on their network, and how to prioritize a response, driven by their own approach to security and risk. As several participants have put it, an SBOM offers a **"roadmap for the defender,"** particularly when it comes to vulnerabilities that might be linked to widespread exploitation and automated tools such as Metasploit.

Alerts about potential end-of-life

Careful understanding of third party components can enable **alerts about potential end-of-life (EOL)** situations. By combining data from SBOMs with other data sources, an organization can understand when a component may no longer be supported by its supplier. This will allow that organization to understand the potential ripple effects for the software using those components, and make proactive decisions to work with their supplier or seek alternatives.

Better support compliance and reporting requirements

More information about components can **better support compliance and reporting requirements**. In addition to being a more detailed asset inventory, SBOMs support a requirement to monitor for security risks of deployed systems (e.g. "post-market surveillance") or a requirement to follow up on security alerts to demonstrate vigilance.

Reduce costs through a more streamlined and efficient administration

Documented software components can **reduce costs through a more streamlined and efficient administration**. Those responsible can quickly identify points of concern, and would not have to spend time contacting suppliers when they can determine via the SBOM that the software does not contain a deficient component.

Ecosystem, Network Effects, and Public Health Benefits of SBOM

While this document is focused on benefits to a specific team, role, or organization, there are significant near-term and subsequent benefits which emerge for the entire ecosystem.

Everyone is potentially a link in a supply chain, and across the entire supply chain benefits are unlocked or enhanced as more links participate.

Just as mass vaccinations of children protects other unvaccinated children via “herd immunity”, each of the links benefit from a greater participation by other links in the supply chain.

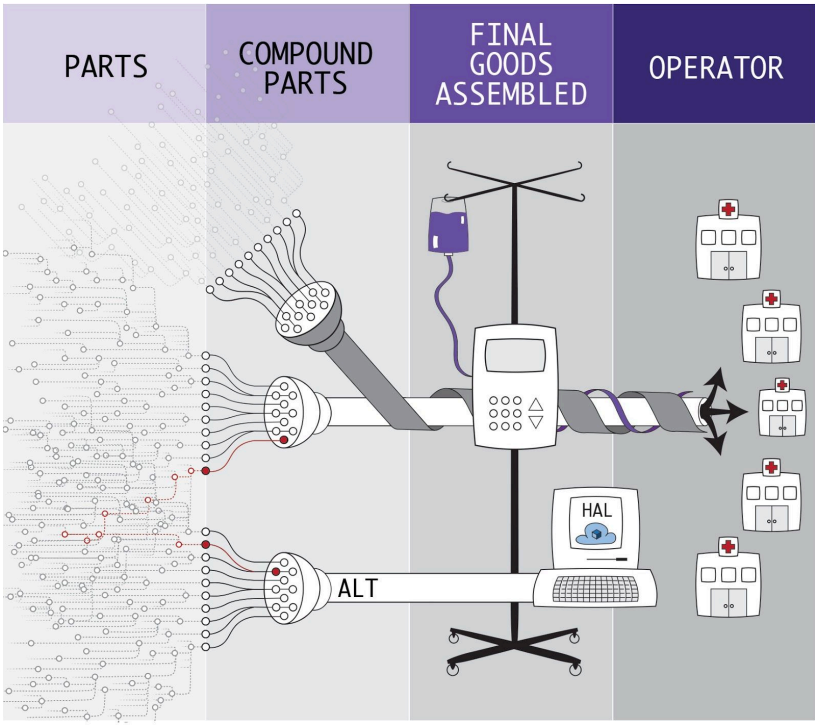


Figure 1: Software Supply Chain Ecosystem

Each of the three perspectives outlined above — *produce, choose,* and *operate* — considers the software supply chain as a single narrowly focused stakeholder might see it. In practice, people and organizations serve multiple roles at any given time, and all stakeholders seek additional benefits from broader, ecosystem-level changes, akin to the effects of vaccination and public spending on population health.

This section explains how SBOM adoption can accelerate positive trends and encourage good practices that improve the health of the entire software ecosystem.

Several of the following ecosystem-level benefits are described in more detail below:

- Accelerated vulnerability management
- Amplified “herd immunity”
- Selecting for better suppliers
- Weathering suppliers going away
- Combined/Cumulative Value

Accelerated Vulnerability Management

In the words of a software operator interviewed for this project, “We need to know what we’re defending.”

Time is of the essence in vulnerability management, but the timeline for fixing deployed systems can stretch into months or years when each stakeholder must wait for disclosure from its upstream suppliers. Accurate SBOMs can collapse this chain of delays to allow all stakeholders to begin assessing vulnerabilities immediately and measure remediation performance throughout the supply chain. The following graphic illustrates this effect.

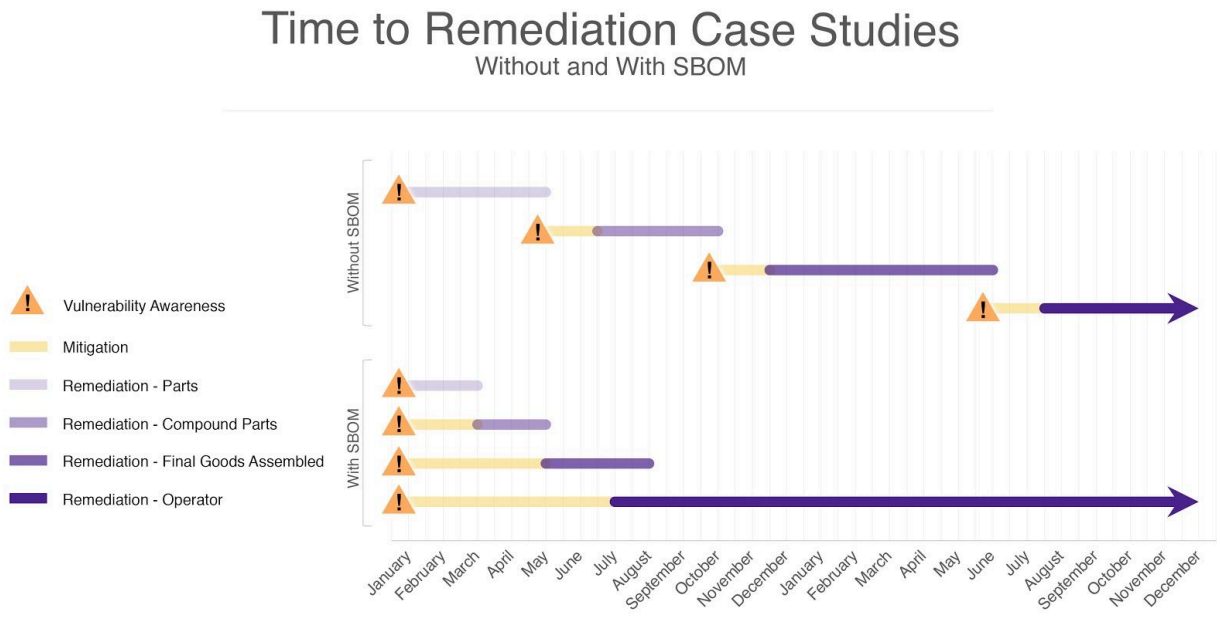


Figure 2: Time to Remediation Case Studies - With and Without SBOM

Upon the revelation of a new vulnerability, the time-to-exploitation is measured in *days* or *weeks*. In contrast, defenders measure the time-to-remediation in *months* and *years,* in large part due to the hierarchical depth of a supply chain. More comprehensive supply chain transparency supports earlier identification, simultaneously, at each stakeholder type including Compound Parts, Final Goods Assemblers, and Operators.

When Defenders are armed with this advanced visibility into the supply chain, workarounds, mitigations, and other corrective actions can significantly compress the time period to enacting corrective actions. Of additional value, downstream dependents, armed with the moment-zero time marker, can begin to measure relative response times of their suppliers for future supplier choices (See section: “Selecting for better suppliers”).

For example, The case of a medical device vulnerability where a Compound Parts supplier took six months to identify, code, test, and discreetly disclose patches to dozens of dependent medical device makers (Final Good Assemblers). Those medical device makers took on average an additional 6 to 12 months each to integrate; test; and apply patches.

Because of these upstream delays, even skilled, well-staffed healthcare teams can take nine months to begin deploying updates. 12–18 months is a more typical timeframe in healthcare. With the improvements brought about through the use of SBOMs, each link of the supply chain could become aware of new vulnerabilities at the same time. Workarounds and mitigations could be put into place immediately while long-term fixes are under development.

NOTE: This opportunity is even further super-charged in combination with benefits of NTIA's other Coordinated Vulnerability Disclosure working groups[4] where initial patches have been made available prior to any adversary awareness.

Amplified "Herd Immunity"

The notion of herd immunity refers to the idea that coordinated *preventive* activities can reduce the risk to individuals in a group, thereby reducing risk to the group overall.

If a single Compound Parts manufacturer avoids a known-vulnerable version of an open source library in favor of a version that is not vulnerable, then their downstream Final Goods Assemblers are also not vulnerable, as are each of their customers. This initial work by a developer could take minutes, or even less with automated tooling, to avoid a known vulnerability, creating what Deming would call "better supply."

This leverages a multiplicative relationship, for example, if a single Compound Goods manufacturer avoids a vulnerable library its downstream qty: 100 Final Goods assemblers will not be vulnerable, which conveys this lack of a vulnerable library to their qty: 100 customers, resulting in an avoidance of a vulnerability to 10,000 Operators.

Selecting for Better Suppliers

"You cannot manage what you cannot measure. You cannot protect what you do not know you have." The inverse of this is a more pervasive transparency unleashing better measurement, analysis, and evolutionary continuous improvement.

Inclusion of low-quality or abandoned software components in products is a recurring problem that can be addressed in part through increased transparency. Some industries, including

[4] A summary of stakeholder-drafted work on CVD, with links to the document is available here: https://www.ntia.doc.gov/blog/2016/improving-cybersecurity-through-enhanced-vulnerability-disclosure

healthcare, are already standardizing mechanisms that allow suppliers to offer extra product details via self-reporting, and buyers are beginning to express strong preferences during procurement. Increased transparency throughout the supply chain can support a process similar to natural selection, wherein resource allocation favors the most “fit” entities and culls those that are not able to compete effectively. In Deming’s words with respect to Toyota’s supply chain, the goal is to “use fewer and better suppliers of parts.”

When Financial Services began Deming-style Software Supply Chain management around 2013, they began to understand and implement metrics for continuous improvement. For example, armed with moment-zero of an open source flaw, what is the Mean-time-to-Remediate (MttR) for Final Goods Assembler A versus B? If Vendor B is consistently fixing new CVEs within 30 days, but vendor A is taking 9 months, Vendor B is likely to get more budget in future procurement. This scales as it is applied across the entire supply chain. If links are required to produce increasingly comprehensive SBOMs by potential downstream links and customers, then Projects may have to migrate from Open Source projects who can’t or won’t supply SBOMs toward projects that will provide SBOMs (See Appendix II for more information). Further, if there are 10 logging frameworks one might choose from, those with the best Mean-time-to-Respond will increasingly win a larger share of adoption and/or funding from initiatives devoted to promoting better security.

SBOMs can help stakeholders determine the relevance of disclosed vulnerabilities, in some cases before their suppliers notify them. In this way, transparency brings to light information that can be used to establish performance metrics, such as time to notification or time to remediation of a vulnerability.

Suppliers that fail to update vulnerable components promptly, or projects that stop updating in response to vulnerabilities, can be exposed to extra scrutiny and have resources allocated away from them over time and across the supply chain.

Weathering Suppliers going away

Increased transparency via SBOM can help stakeholders address the acute problem of supplier extinction. Given a process that supports the selection of better software over time (See section: “Selecting for better suppliers”), a natural consequence is that not all elements of the supply chain will survive; this can be thought of as supply extinction. Inevitably, companies go out of business or are acquired, re-acquired, and abandoned. Even at healthy, sustainable companies, product lines reach End of Life (EOL). And open source projects lose momentum or maintainers.

In today’s software supply that generally operates without SBOM, dependents may be wholly reliant on suppliers to notify them of new vulnerabilities. In cases of supplier extinction, there may be no notification - or the notification may be a headline of active exploitation and harm in

the wild. In contrast, a user of an SBOM-enabled component is better informed and empowered to make appropriate decisions. Without needing a direct communication from the supplier about EOL status, each downstream user can self-assess potential impact, irrespective of the financial health or current name/brand of the original creator.

Some industries can use existing trust networks to become collectively more resilient to supply extinction. Trusted third parties such as industry information sharing & analysis centers (ISACs) that already play central roles can collect SBOMs to ease the burden of information management across suppliers and operators. Regulated industries such as healthcare could more swiftly issue notifications about vulnerable devices, even long after the device maker was no longer in existence.

Cumulative Value

The benefits of accelerated vulnerability management, amplified herd immunity, selecting for better suppliers, and weathering suppliers going away reinforce each other for greater cumulative effect. Promoting an ecosystem with these characteristics will lead to safer systems with fewer, more manageable risks, and compounding benefits throughout the supply chain.

Opaque, weaker, vulnerable systems contribute to *herd vulnerability*; more transparent, resilient, and maintainable systems contribute to *herd immunity*. Herd immunity makes systems less prone to accidents and adversaries.

At every supply chain level, the shift from herd vulnerability to herd immunity highlights the cumulative, public health-like benefits of the added transparency and resiliency unlocked by SBOMs. For suppliers, transparency and resiliency are increasingly necessary because of the increasing complexity of supply chains. Suppliers who embrace these efforts can contribute, higher quality, better maintained projects. This added transparency and resiliency offers developers the opportunity to select only the most diligent suppliers and their least vulnerable versions to be included in their software. In turn, Compound Parts and Final Goods Assembled will be higher quality and more easily maintained as a result. For Purchasers, this enables timely and thorough reviews of products and systems. Subsequently for Operators, increased transparency results in more manageable risk and more maintainable, better quality Final Goods in the operating environment.

As these practices become more pervasive, their cumulative benefits further enhance the role specific and stakeholder specific benefits. The “public health”, system-wide, network effects also dramatically improve “patient health” for you and those dependent upon you.

Appendix I Related efforts that explicitly or implicitly highlight the value of SBOM

The work of the NTIA initiative does not occur in a vacuum. There are a number of key works across the ecosystem that have advanced or highlighted the importance of an SBOM at various points in the supply chain. The following is a list of related projects that are included to emphasize the growing support and importance of SBOM. It is not an exhaustive list and the projects below are not endorsed by this group.

BSA Framework for Secure Software.
This industry-drafted framework[5] offers guidance on secure development of software, security capabilities of the software, and a secure lifecycle, citing standards and other authoritative guidance. It makes repeated references to the importance of tracking third party code, including advising “To the maximum feasible through the use of manual and automated technologies, subcomponents integrated into third party components are documented, and their lineage and dependencies traced.”

Building Security in Maturity Model
BSIMM (Building Security in Maturity Model) is a large group of software developers in academia, government, and industry that benchmark best software development practices. They create practices that organizations can benchmark themselves against and assess where they are relative to their peers in their industry or overall. Version 9 of the BSIMM[6] contains several SBOM related requirements:

SR2.4 "Identify open source"
SR3.1 "Control open source risk"
CMVM2.3 "Develop an operation’s inventory of applications"
SFD3.2 "Require use of approved security features and frameworks"
SE3.6 "Enhance application inventory with operations bill of materials"

CISQ Trustworthy System Manifesto
The Council on IT Software Quality (CISQ) has published the “CISQ Trustworthy System Manifesto”[7] on holding senior executives accountable for cybersecurity. Section III is "Traceable

[5] The BSA Framework for Secure Software
https://www.bsa.org/files/reports/bsa_software_security_framework_web_final.pdf
[6] BSIMM9
https://www.bsimm.com/content/dam/bsimm/reports/bsimm9.pdf
[7] CISQ Trustworthy System Manifesto
https://www.it-cisq.org/trustworthy-systems-manifesto/index.htm

Properties of System Components" which has requirement #2 “Evidence of provenance and trustworthiness should be carried forward with components and shared across the supply chain” which contains in the description:

> “When developers incorporate open source components, external APIs, or microservices, they should document their source and related data for inclusion in a System Bill of Materials (SBOM)."

FDA Premarket Guidance

The US Food and Drug Administration (FDA) has published draft Pre-Market Guidance[8] for medical device manufacturers seeking FDA certification. This guidance maintains that: "The device design should provide a CBOM in a machine readable, electronic format to be consumed automatically" where Cybersecurity Bill of Materials (CBOM) is defined as "a list that includes but is not limited to commercial, open source, and off-the-shelf software and hardware components that are or could become susceptible to vulnerabilities."

FS-ISAC Third Party Governance

The Financial Section Information Sharing and Analysis Center (FS-ISAC) published “Appropriate Software Security Control Types for Third Party Service and Product Providers” in 2015. It includes Control Type 3B, “A Bill of Materials (BOM) for Commercial Software to Identify Open Source Libraries Used”.[9]

ISO

ISO/IEC 27002:2005 and 27002:2013 have relevant sections that highlight the importance of best practices to ensure adherence to information security control objectives for an organization. The perspectives identified in this document can be aligned with this international standard to show its relevance to a broad number of industries that use/produce information systems.

Make Software	ISO/IEC 27002:2005, 9.2.6, “Secure Disposal or Re-use of Equipment”; Section 10.4, “Protection against Malicious and Mobile Code”; Section 15.1.2. “Intellectual Property Rights(IPR).” ISO/IEC 27002:2013, Section 14: System acquisition, development and maintenance - 14.2 Security in development and support processes

[8] FDA Cybersecurity Guidance and Safety Communications https://www.fda.gov/medical-devices/digital-health/cybersecurity#guidance

[9] Financial Services ISAC Third Party Software Security Working Group. “Appropriate Software Security Control Types for Third Party Service and Product Providers” Version 2.3 was published in October, 2015. https://www.fsisac.com/

Choose Software	ISO/IEC 27002:2013, Section 14: System acquisition, development, and maintenance 15: Supplier relationships - 15.1 Information security in supplier relationships
Operate Software	ISO/IEC 27002:2005, Section 5.1.1, "Inventory of Assets." and Section 10.4, "Protection against Malicious and Mobile Code"; Section 15.1.2. "Intellectual Property Rights(IPR)." Section 9.2.7, "Removal of Property"; Section 9.2.6, "Secure Disposal or Re-use of Equipment"; Section 10.7.2, "Disposal of Media." Section 13.2, "Management of Information Security Incidents and Improvements"; Section 10.10.2, "Monitoring System Use"; Section 15.2.2, "Technical Compliance Checking";

Table 2: SBOM Perspectives and Related International Standards

Linux Foundation OpenChain

The Linux Foundation OpenChain[10] project is on the use of open source and contains: "A process exists for creating and managing a FOSS component bill of materials which includes each component (and its Identified Licenses) from which the Supplied Software is comprised"

Manufacturers Disclosure Statement for Medical Device Security

The Manufacturer Disclosure Statement for Medical Device Security (MDS^2)[11] was originally developed by the Healthcare Information and Management Systems Society (HIMSS) and the American College of Clinical Engineering (ACCE), and then standardized through a joint effort between HIMSS and the National Electrical Manufacturers Association (NEMA). The MDS^2 form provides medical device manufacturers with a means for disclosing to healthcare providers the security related features of the medical devices they manufacture.

[10] OpenChain Specification Version 2
https://wiki.linuxfoundation.org/_media/openchain/openchainspec-current.pdf

[11] Manufacturer Disclosure Statement for Medical Device Security
https://www.nema.org/Standards/Pages/Manufacturer-Disclosure-Statement-for-Medical-Device-Security.aspx

MITRE Deliver Uncompromised
MITRE, in its report on the national security supply chain, “Deliver Uncompromised”[12] recommends SBOMs as part of supply chain integrity. It notes, “If done properly, an SBOM can estimate the overall risk of the ensemble of software elements based on the risk of the individual elements.”

NIST’s Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF)
A 2019 draft white paper[13] recommends a core set of high level secure software development practices. Among these, it recommends that organizations seeking to protect their software “Create and maintain a software bill of materials (SBOM) for each piece of software stored in the repository.”

OWASP Component Analysis Project
This industry expert group’s guidance on component analysis[14] recommends “Contractually require SBOMs from vendors and embed their acquisition in the procurement process” and a list of best practices using the SBOM to improve security

SAFECode Managing Security Risks Inherent in the Use of Third party Components
Industry group SAFECode drafted a white paper[15] capturing the collective knowledge on the benefits and challenges of managing third-party code risk in product development.

Software Heritage
Software Heritage[16] is a non-profit initiative actively supported by a large number of organizations[17] —software, systems and tool vendors, IT users, academic and governmental institutions. It is building a universal archive of software source code, as a common infrastructure catering to a variety of use cases from industry to science and culture.

[12] MITRE Deliver Uncompromised
https://www.mitre.org/publications/technical-papers/deliver-uncompromised-a-strategy-for-supply-chain-security
[13] NIST White Paper (Draft): Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF)
https://csrc.nist.gov/publications/detail/white-paper/2019/06/11/mitigating-risk-of-software-vulnerabilities-with-ssdf/draft
[14] OWASP Component Analysis
https://www.owasp.org/index.php/Component_Analysis#Software_Bill-of-Materials_.28SBOM.29
[15]SAFECode White Paper: Managing Security Risks Inherent in the Use of Thirdparty Components
https://safecode.org/wp-content/uploads/2017/05/SAFECode_TPC_Whitepaper.pdf
[16] Building the Universal Archive of Source Code
https://cacm.acm.org/magazines/2018/10/231366-building-the-universal-archive-of-source-code/abstract
[17] Software Heritage Testimonials
https://www.softwareheritage.org/support/testimonials/

One of the use cases specifically listed on their mission statement is source code tracking for industry[18]:
"*Because industry cannot afford to lose track of any part of its source code, we track software origin, history, and evolution. Software Heritage will provide* ***unique software identifiers, intrinsically bound to software components****, ensuring persistent traceability across future development and organizational changes.*"

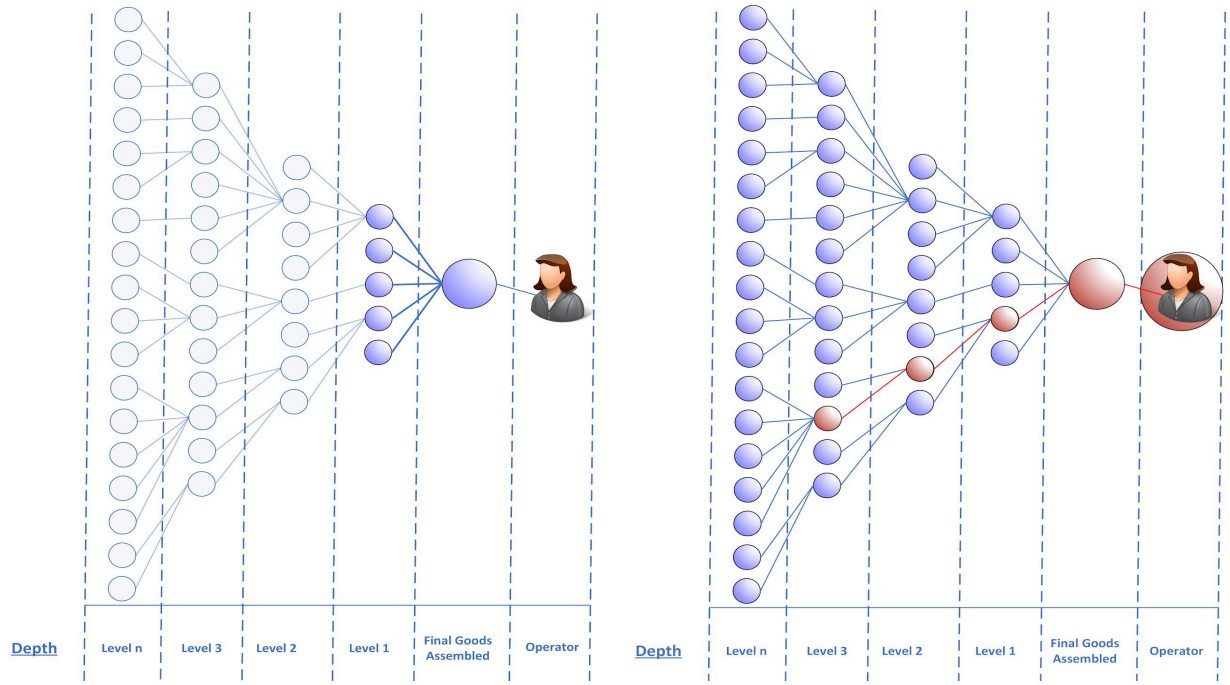
These intrinsic identifiers are based on cryptographic signatures, have a precise formal definition[19] and are already available for the more than 10 billions of artifacts stored in the Software Heritage archive[20]. They are an essential building block for ensuring the **integrity** of a source code base and are currently being used by some major industry players to implement a part of their SBOM workflow, related to source code distribution obligations[21], as well as from the Wikidata community[22].

[18] Software Heritage Mission Statement: An essential infrastructure for industry
https://www.softwareheritage.org/mission/industry/
[19] Software Heritage: Precise identifiers
https://docs.softwareheritage.org/devel/swh-model/persistent-identifiers.html#persistent-identifiers
[20] Software Heritage: Archive
https://archive.softwareheritage.org
[21] Outsourcing Source Code Distribution Requirements
https://archive.fosdem.org/2018/schedule/event/outsourcing_distribution_requirements/
[22] SWH Release ID
https://www.wikidata.org/wiki/Property:P6138

Appendix II - SBOM Depth vs Effectiveness

Depth considerations

Completeness of visibility into the supply chain is the strategic goal. The depth of a dependency tree is often a practical consideration of completeness and/or effectiveness - especially in complex multi-component systems of technology. Having insight into even just one level of suppliers is greater than zero, but more complete SBOMs support more use cases and greater percentages of transparency. The “Framing Software Component Transparency” document[23] outlines both the minimum expectations for 1-hop SBOMs and approaches to recursion for completeness. Below is an illustration of the importance “more than 1-hop”. In some supply chain analysis, direct dependencies were less than 10% of the complete list of dependencies. Further, an increasing number of attacks target popular atomic parts or compound parts - quite shallow in the attack surface for adversaries, but quite deeply hidden to defenders in opaque, complex supply chains. In these cases, 1-hop SBOMs may cause a false sense of security.



Limited visibility enables less awareness of risk

More complete visibility enables more complete awareness of risk

Figure 3: Illustration of SBOM Depth (1-hop vs Many-hops)

[23] See Framing Software Component Transparency at https://ntia.gov/SBOM.

An example of a need for an SBOM with depth (> 1 hop)

While writing this document, a helpful example emerged illustrating the need for listing more than 1 level of dependencies/suppliers. A batch of vulnerabilities affecting many safety critical systems was dubbed “Urgent/11” in the summer of 2019. The initial vulnerability finders identified that the flaws were present in certain versions of Wind River’s VxWorks RTOS (Real Time Operating System). In response, Wind River provided thorough impact analysis of their affected versions of VxWorks[24]. SBOMs with direct suppliers like the affected VxWorks versions are *helpful* as dependent hospitals could answer: *“Am I affected? Where am I affected?”* - but only partially. It was later revealed that the actual vulnerabilities were from a supplier to Wind River - named IPnet (whose creator, Swedish company Interpeak, was later acquired by Wind River.)

With later revelations, we now know that multiple other technology providers and other RTOS vendors were also affected, including ENEA, Green Hills, Microsoft, Mentor, TRON Forum, and IP Infusion - thus exposing many other medical device makers (and other systems). Hospitals only receiving 1-hop SBOMs could be impacted by others who use the included vulnerable IPnet code. The FDA raised this example in the September 2019 NTIA meeting as to why SBOMs must be as complete as possible. In October 2019, both FDA[25] and DHS[26] published expanded lists of known products affected by these IPnet flaws. In the current state of very little supply chain transparency, full discovery will continue to take time - and may only be possible after harm. Conversely, in a world with more vendors providing SBOMs as well as more complete SBOMs, dependent stakeholders can more effectively and rapidly manage their risks.

To tie this example to some of the NTIA SBOM nomenclature, Urgent/11 revealed flaws in versions of a *Compound Part* called VxWorks. Large numbers of *Final Goods Assembled* medical devices were affected by this shared *Compound Part*. Subsequently, *Operators* in hospitals wished to determine: “Am I affected? Where am I affected?”. (See Figure 1 above) Some medical device makers who tracked and supplied only a “1-hop” direct list of suppliers would be able to successfully answer those questions and enable these hospital *Operators* to manage those risks. However, when it was later revealed that the flaws were in IPnet - an upstream *Part* to the VxWorx *Compound Part*, “1-hop” SBOMs would prove insufficient - missing a larger and growing list of technologies (See Figure 3 above). Appendix III details such use cases and a path to address the increasing need for transparency and clarity with SBOMs.

---

[24] SECURITY VULNERABILITY RESPONSE INFORMATION TCP/IP Network Stack (IPnet, Urgent/11) https://www.windriver.com/security/announcements/tcp-ip-network-stack-ipnet-urgent11/

[25] URGENT/11 Cybersecurity Vulnerabilities in a Widely-Used Third-Party Software Component May Introduce Risks During Use of Certain Medical Devices: FDA Safety Communication https://www.fda.gov/medical-devices/safety-communications/urgent11-cybersecurity-vulnerabilities-widely-used-third-party-software-component-may-introduce

[26] ICS Advisory (ICSA-19-211-01) Wind River VxWorks https://www.us-cert.gov/ics/advisories/icsa-19-211-01

Appendix III - Assurance and Confidence Use Cases and Elements of an SBOM

The basic SBOM described in this document and related efforts can offer many benefits, as discussed above. However, some use cases may require more information about the software or the SBOM itself. Beyond component identities, supply chain stakeholders may want to know more information including: the integrity of the components, the pedigree of their creators, how the components were assembled, and how the SBOM itself was compiled. Higher assurance organizations may want these further elements as they could suffer dire consequences from allowing maliciously altered or contaminated software.

Provenance

The **Provenance** of an SBOM is the term of art for having information about the chain of custody of the software and all of the constituent components that comprise that software, capturing information about the authors and locations from where the components were obtained. Whether a component comes directly from the supplier's distribution site or some other location can be a concern for some organizations. Similarly, understanding the exact identity of the supplier can help an organization establish where to go for updates or to communicate about bugs or enhancements. Finally, access to authorship allows organizations to correlate their experience with components to the creators and rank their internal preferences through reputation-like scoring of providers of software.

Pedigree

The **Pedigree** of an SBOM is the term of art for having information on all of the components that have come together to make a piece of software and process under which they came together. This can include details beyond components, such as compiler options. For example, understanding whether compilation options invoking ASLR were used or not used indicates that the resultant piece of deployable code is hardened against certain types of attacks. Understanding of the process used in taking the source code and incorporated components and libraries to formulate the resultant executable is an important source of insight for those who need to know what selection of options were used in creating the executable software.

Integrity

The **Integrity** of the SBOM refers to the use of cryptographic techniques to indicate that the SBOM hasn't been altered since written by its author or if there was a modification it indicates

that alteration by some subsequent SBOM author. Being able to determine the SBOM's integrity can help, for example, in situations where there is concern about whether an adversary may be purposefully trying to alter the SBOM to mislead those using them for analysis of vulnerabilities. If someone edits the SBOM to indicate it has a later, non-vulnerable version of a component, the organization will be left susceptible to attacks against that vulnerability even though the altered SBOM indicates they are using a non-vulnerable version. Similarly, alteration of the authorship or source information would undermine the Provenance of the SBOM or alteration of the details of the formulation choices would undermine the Pedigree of the SBOM.

These three SBOM features can supplement the benefits above to provide concrete security benefits, particularly for organizations that face active threats to their supply chain from determined adversaries. Future work will explore these potential SBOM use cases, and map them to specific elements.

Appendix IV - About the authors of this document

This document was drafted by an open working group convened by the National Telecommunications and Information Administration in a multistakeholder process, including the following individuals and organizations:

- John Banghart (Venable)
- Justine Bone (MedSec)
- Slava Bronfman (Cybellum)
- Josh Corman (PTC)
- Roberto Di Cosmo (Software Heritage / Inria)
- Allan Friedman (NTIA)
- Christopher Gates (Velentium)
- Charlie Hart (Hitachi)
- Audra Hatch
- Kent Landfield (McAfee)
- Art Manion (SEI)
- Bob Martin (MITRE)
- Mike Powers (Christiana)
- Ben Ransford (Virta Labs)
- Vijay Sarvepelli (SEI)
- Duncan Sparrell (sFractal Consulting)
- Tim Walsh (Mayo Clinic)

Others participated, but do not wish to be named. Input into this document included numerous interviews, creation of use cases, and input from the Healthcare PoC, as well as regular presentations to the broader NTIA-convened community.