TLP:CLEAR

INL/RPT-23-71296
Revision: 0

U.S. DEPARTMENT OF ENERGY
*Office of* Cybersecurity, Energy Security, and Emergency Response

# Software Bill of Materials (SBOM) Sharing Lifecycle Report

Publication: April 2023

*This page is intentionally left blank.*

## DISCLAIMER

This document is marked TLP:CLEAR. Disclosure is not limited. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be distributed without restriction. For more information on the Traffic Light Protocol, see http://www.cisa.gov/tlp/.

## ACKNOWLEDGEMENTS

This work was co-sponsored by the U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) and the U.S. Department of Energy (DOE) Cybersecurity, Energy Security, and Emergency Response (CESER).

CISA is a new agency in the federal government, established in 2018 to be America's Cyber Defense Agency. CISA serves as the national coordinator for critical infrastructure security and resilience, leading the effort to understand, manage, and reduce risk to the cyber and physical infrastructure that Americans rely on every hour of every day.

As the majority of the nation's critical infrastructure is owned and operated by the private sector, operational collaboration is foundational to CISA's efforts. CISA works with a wide array of partners across the globe—from every industry; to federal, state, local, tribal, territorial, and international governments; to non-profits; academia; and the research community—connecting them together and to the resources, tools, and information that will help them fortify their security and resilience against current and emerging threats.

The mission of DOE CESER is to lead DOE's efforts to enhance the security and resilience of U.S. critical energy infrastructure to all hazards, mitigate the impacts of disruptive events and risk to the sector overall through preparedness and innovation, and respond to and facilitate recovery from energy disruptions in collaboration with other federal agencies, the private sector, and state, local, tribal, and territorial (SLTT) governments.

As part of this mission, CESER leads DOE's preparedness and emergency response efforts across the entire energy sector, including electricity, oil, natural gas, and renewables. These efforts include the development of energy security and resilience policies at the federal and SLTT levels; capacity building activities such as exercises, training, and workforce development; risk analysis initiatives; research, development, and demonstration activities to mitigate cyber-, physical-, and climate-based risks; and emergency response activities in partnerships with industry, the SLTT community, and interagency partners such as the Federal Emergency Management Agency (FEMA) and CISA from all hazards.

CISA and DOE CESER would like to thank the following authors, contributors, and reviewers for their dedication and commitment to the development of the Software Bill of Materials (SBOM) Sharing Lifecycle Report:

## AUTHORS

Jeremiah Stoddard (INL), Critical Infrastructure Analyst

Michael Cutshaw (INL), Critical Infrastructure Analyst

Tyler Williams (PNNL), Cyber Security Engineer

Allan Friedman (CISA), Senior Advisor and Strategist

Justin Murphy (CISA), Vulnerability Analyst

## CONTRIBUTORS

Heather Rohrbaugh (INL), Writer/Editor

Jessica Smith (PNNL), Senior Cyber Security Researcher

Jeremy Jones (INL), Critical Infrastructure Analyst

Animesh Pattanayak (PNNL), Cyber Security Researcher

Bianca Steele (PNNL), Cyber Security Engineer

Virginia Wright (INL), Cyber-Informed Engineering Program Manager

Jeffrey Mitchell (INL), Project Manager

Will Woodworth (CISA), Vulnerability Analyst

## REVIEWERS

Megan Kommers (INL), Analytic Manager

Timothy Klett (INL), Senior Technology Integration Strategist

Julia Townsend (INL), Project Coordinator

Megan Doscher (CISA), Section Chief, Technology Assurance

Stephanie Johnson, Ph.D., (DOE CESER), Program Manager, Supply Chain Cyber Risk Management

# LIST OF ACRONYMS

| | |
|---|---|
| API | Application Programming Interface |
| CISA | Cybersecurity and Infrastructure Security Agency |
| HTTP/S | Hypertext Transfer Protocol/Secure |
| MUD | Manufacturer Usage Description |
| NTIA | National Telecommunications and Information Administration |
| REST | Representational State Transfer |
| SBOM | Software Bill of Materials |
| SOAP | Simple Object Access Protocol |
| URL | Uniform Resource Locator |
| VEX | Vulnerability Exploitability eXchange |

## EXECUTIVE SUMMARY

As Software Bill of Materials (SBOM) adoption efforts mature, SBOM sharing continues to occur, but no single solution or set of solutions have become ubiquitous. The purpose of this report is to enumerate and describe the different parties and phases of the SBOM sharing lifecycle and to assist readers in choosing suitable SBOM sharing solutions based on the amount of time, resources, subject-matter expertise, effort, and access to tooling that is available to the reader to implement a phase of the SBOM sharing lifecycle.

The SBOM sharing lifecycle consists of the Discovery, Access, and Transport of an SBOM, and this report details these individual phases and how an SBOM goes from author to the consumer. This report also details how potential enrichment activities may be performed on an SBOM to create a new product before or after it has been shared. The concept of a sophistication classification for SBOM sharing solutions is concurrently introduced with a focus on the inclusion or lack of certain features and effort associated with their implementation. Examples of low, medium, and high-sophistication solutions are provided; however, these examples and associated categorizations should not be seen as a qualitative judgment meant to push the reader toward a particular adoption strategy since sharing solutions are chosen based on the unique needs of the user. This report does recommend the SBOM community consider how to make current and future sharing solutions interoperable with each other as well as more automated methods to facilitate sharing and broader SBOM adoption.

This report also highlights SBOM sharing survey results obtained from interviews with stakeholders to understand the current SBOM sharing landscape. The categorized results of the survey suggest that SBOMs are currently transported directly to the receiver through email or similar informal communication mechanisms or alternatively the SBOM resides on a repository available to consumers. In addition to these transport methods, this report captures industry efforts to create private sharing solutions and services that can store and transport enrichment data and may use higher sophistication features that are cloud-based or use distributed ledger technologies.

# CONTENTS

## LIST OF FIGURES



## LIST OF TABLES

# INTRODUCTION

In 2018, collaborative community efforts with Software Bill of Materials (SBOMs) began when the National Telecommunications and Information Administration (NTIA) launched its multistakeholder process.[1]

These efforts led to the creation of working groups[a] that focused on software component transparency. The working groups introduced the associated concepts of SBOM, provided technical resources, created proof-of-concept work, and produced implementation materials. In late 2021, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) began advancing efforts on SBOM through its facilitation of community engagement. These community-led efforts have taken the form of community-created educational documents, related event participation (e.g., SBOM-a-rama,[2] Public Listening Sessions on Advancing SBOM Technology, Processes, and Practices[3]), and new ongoing SBOM-related work streams.[b] One of the new CISA-facilitated work streams focuses on the sharing of SBOMs. This effort is built upon prior stakeholder efforts to provide users with different discovery[c] and access[d] options, and to minimize "the burden on diverse authors and consumers of SBOM data."[4]

The multistakeholder and community-led SBOM efforts have proven fruitful in understanding the current state of SBOM creation, distribution, and consumption. Two things have become clear from these stakeholder engagements: (1) SBOM sharing is currently happening, and (2) no single, ubiquitous solution is being used by all stakeholders.

## Report Purpose

While there has been substantial community discussion on SBOM generation, there have been fewer focused discussions on SBOM sharing. The goal of the report is to highlight the currently used SBOM sharing solutions and assist readers in considering appropriate sharing solutions depending on their needs concerning the discovery, access, and transport of SBOMs.

---

a The NTIA's efforts led to the creation of working groups that focused on framing, awareness and adoption, formats and tooling, and a Healthcare Proof of Concept.

b The community participants of the 2021 SBOM-a-rama identified the areas of potential work that make up the current CISA work streams. The CISA-facilitated listening sessions helped cement the community's consensus to move forward on the following workstreams: cloud and online applications, on-ramps and adoption, sharing and exchanging, and tooling and implementation.

c This paper uses the same definition of Discovery that was published by the NTIA in its "Sharing and Exchanging SBOMs" document found at https://ntia.gov/files/ntia/publications/ntia_sbom_sharing_exchanging_sboms-10feb2021.pdf.

d The NTIA defines Access as "transfer of the SBOM using the method derived from discovery." This paper takes that definition and creates a narrower definition of Access while adding the new term "Transport" to cover the NTIA's broader definition of Access.

## COMMUNITY-LED EFFORTS ON SBOM SHARING

The federal government's multistakeholder[5] and community-led[6] efforts on software component transparency include drafting documents that introduce and assist readers in understanding SBOM implementation, provide technical resources, and document lessons learned from the proof-of-concept work. This consensus-based work and the resulting documents serve as the knowledge base for current SBOM discourse. While these multistakeholder and community-created documents were written with different objectives in mind, many of the documents have overlapping discussions on the sharing of SBOMs.

The current documents that touch on SBOM sharing include content on the creation of a common sharing terminology,[7] a tool taxonomy,[8] and a conceptual SBOM exchange[9] to help readers see the larger SBOM picture, while also helping readers understand that SBOMs may be transmitted in different ways. The documents consider what delivery methods are currently possible with modern development processes, what methods stakeholders can use to accommodate industry adoption time and legacy processes/technologies, and what methods could be used for emerging and high-assurance use cases. These documents are effective in communicating general principles surrounding SBOM sharing but may not be effective in assisting an SBOM stakeholder make customized SBOM sharing decisions based on the resources the user has available. To make these decisions, an SBOM stakeholder must first understand the different interactions that an *author, consumer, or provider* (see definitions in Table 1) may have to share an SBOM.

## TERMINOLOGY

The definitions below in Table 1 expand on previous NTIA SBOM sharing documentation and terminology as well as introduce new terms. One term specific to the following sections is *sophistication* (see definition in Table 1). This was chosen over other terms such as maturity, comprehensiveness, and complexity to characterize that the sharing lifecycle phases can vary based on use case. The sophistication rating is determined based on multiple factors as listed below.

*Table 1. Definitions.*

| Term | Definition |
|---|---|
| **Author** | Creates an SBOM. |
| **Consumer** | Receives the transferred SBOM. This could include roles such as third parties, authors, integrators, and end users. |
| **Provider** | Possesses an SBOM. |
| **Discovery** | Mechanism used by the consumer to know the SBOM exists and how to access it. |
| **Access** | Access control mechanisms used by the author or provider to regulate who can view or use an SBOM. |
| **Transport** | Mechanism provided by the author or provider to transfer an SBOM. Also, the action of the consumer receiving an SBOM. |
| **Enrichment** | Activities that leverage an SBOM to create a new product, which may include the antecedent SBOM. This may be done by an author, consumer, provider, or other third party. |
| **Sophistication** | The relative amount of time, resources, subject-matter expertise, effort, and access to tooling needed to implement a phase of the SBOM sharing lifecycle. Sophistication can be either Low, Medium, or High. |

## SBOM SHARING LIFECYCLE PHASES OVERVIEW

The interaction between relevant parties in the sharing of SBOMs will be referred to as the SBOM sharing lifecycle. The NTIA "Sharing and Exchanging SBOMs" document contains a two-step approach to Advertisement/Discovery and Access.[10] The sharing lifecycle expands on this approach and focuses on the complete process of how SBOMs are shared from author to consumer. The lifecycle consists of the *Discovery, Access, and Transport* phases (see Figure 1 and definitions in Table 1) and represents how an SBOM goes from the author to the consumer. These three phases are used to simplify the potentially complex process of the SBOM lifecycle.


Figure 1. Flow chart of the basic building blocks of the sharing lifecycle.

The author will leverage a discovery method that will enable the consumer to identify the location of an SBOM. In the Access phase, the consumer fulfils any authorization requirements set in place by the provider. After authorization is granted, a transport method is provided to the consumer. If the consumer is the end user of the SBOM, the cycle will be completed after the Transport phase of the SBOM.

An additional step may be taken if the consumer of the SBOM is a downstream author (see Figure 2). The downstream author may perform an enrichment activity and add additional information to the SBOM or create a new product (i.e., incorporating the data into another SBOM to expand its internal-components information). From that point, the sharing lifecycle phases begin again with the downstream author, starting from the author role and sharing the updated information through the Discovery phase.

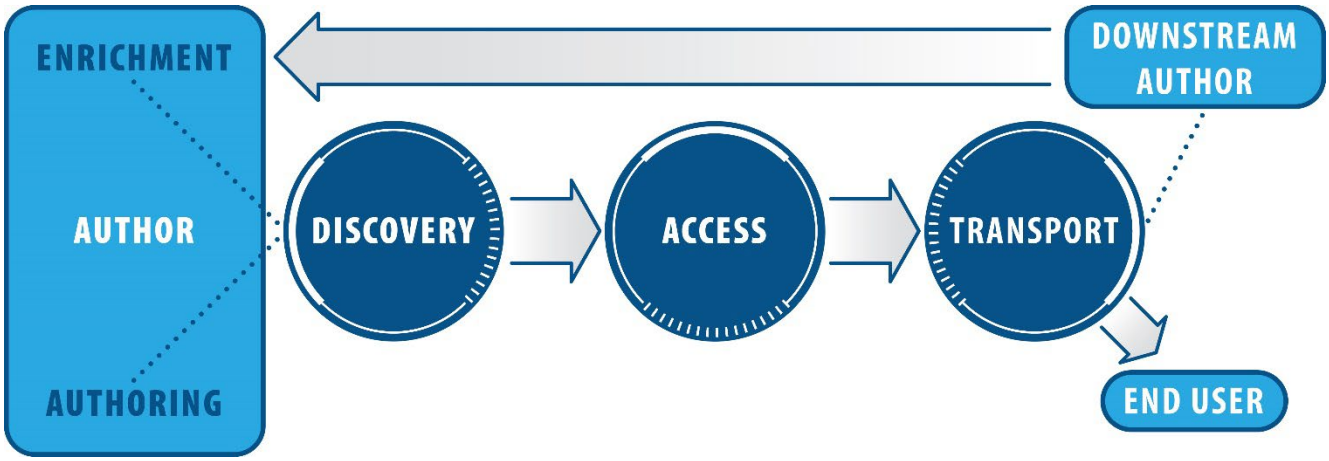


Figure 2. The flow chart expands on the basic steps to help illustrate the potential complexity of the sharing lifecycle.

Each phase contains unique characteristics for consideration and have been separated into sophistication ratings. These ratings can be based on the inclusion or lack of features and effort associated with their implementation.[11] The ratings reflect different features and do not suggest a certain level of sophistication is required as they are use-case specific. Due to the vast interplay of expertise, time, and cost, the rating can be explained through single or multiple aspects. This interplay can lead to small modifications that can increase or decrease the implementation rating.

While these ratings vary with each use case, a consistent trend is the ability to minimize manual interaction between the author and consumer. The next section details the individual phases and each of the ratings, providing example solutions and explaining how they each fit within the rating structure. These examples help provide a starting point when reviewing potential solutions for a use case.

## SBOM SHARING LIFECYCLE PHASES DISCUSSION

The purpose of Table 2 is to highlight possible examples of sophistication for each SBOM's lifecycle phase. The uneven distribution of features represents that some sophistication levels are characterized by the lack of certain features or simply act as a middle ground between high and low.

*Table 2. SBOM sharing lifecycle sophistication examples.*

| Lifecycle Phase | Sophistication - Low | Sophistication - Medium | Sophistication - High |
|---|---|---|---|
| **Discovery** | • Consumer initiated<br>• Limited or non-existent guidance given by Provider | • SBOM placed in software source code<br>  – Point in time (Singular version)<br>  – Manufacturer Usage Description (MUD)<br>• Known central repository<br>• Website | • Automated propagation of available SBOMs<br>• Continuous updates to relevant parties<br>• Publish/Subscribe pattern<br>• Distributed ledger |
| **Access** | • No controls in place<br>• Manual controls<br>• Case-by-case | • Authentication required<br>• Limited access control granularity<br>• Private/broadcast/public channels, roles<br>• Private chains/consensus algorithm | • Delegated authentication and access controls<br>• Full access control granularity |
| **Transport** | • Human-initiated process<br>• Point-to-point<br>• Verbal transmission | • Inconsistent, varied method or documentation<br>• Ad-hoc automation | • Documented<br>• Repeatability<br>• Automated access<br>• Well-known protocols (e.g., REST/RESTful/ SOAP API)<br>• Distributed ledger synchronization |

## Discovery

The initial phase of the lifecycle involves how a consumer will gain awareness of the existence of an SBOM from an author or provider. The SBOM could be discoverable through a standardized placement within a vendor website or location within software source code. Sufficient guidance should be provided to enable the continuation into the Access and Transport phases. The Discovery phase should also clearly state if the SBOM requires the consumer to continuously contact the provider and request updates. Alternatively, continuous updates could be provided through an automated process.

### *Discovery – Low Sophistication*

The low-sophistication features of the Discovery phase describe a solution in which the provider does not prepare any major mechanisms to assist interested parties in locating an SBOM. This places the burden of the Discovery phase on interested parties, and the consumer will likely need to manually search a vendor website that is not explicitly known to contain SBOMs. The consumer may have to reach out through different contacts, email various representatives, or otherwise engage in a possibly lengthy and multistep process to obtain information about where an SBOM may reside. This flow may follow a different path for anyone who attempts to discover an SBOM. In the low-sophistication Discovery phase, the search is highly manual and does not present major opportunities for automation.

### *Discovery – Medium Sophistication*

To reach medium sophistication, a provider's SBOM location and access procedures may have some well-known aspects. For example, a provider who distributes code may place an SBOM within the software source code. This location makes it simple for a consumer who is interested in that singular version, but instructions for obtaining new or past versions of the SBOM may not be present.

A provider may have a company or organizational website, which is promoted or easily searchable. This website, among other purposes, can distribute SBOMs. It is assumed that for medium sophistication, there may be some guidance on how to reach the portion of such application that is able to distribute SBOMs, but some navigation by the consumer is still needed.

### *Discovery – High Sophistication*

For a high-sophistication approach, the burden of discovery is placed more heavily on the provider to lessen the effort exerted by the consumer. There may be a well-known and documented process that is ripe for automation and has few aspects that require manual intervention. For example, a provider may create a publish/subscribe service that will provide automatic updates about new SBOMs, updated versions of existing SBOMs, and provide some mechanism that describes where they may be found. In addition, higher levels of sophistication should have an increased amount of precision in guiding consumers towards requested information without displaying irrelevant information.

## Discovery Solution Examples

This section serves to provide examples of how the various sophistication levels could be applied to different types of solutions regarding the Discovery phase.

### Email

A low-sophistication implementation of email would be if the consumer needs to directly email the author to determine if an SBOM exists, and how it might be obtained. This is a low-sophistication example as the consumer does not have enough information to know if an SBOM exists and how it might be accessed; therefore, the consumer must manually reach out to obtain the needed information. In addition, such a process is not immediate as the author may have some delay before providing a response and it may take multiple communications with the consumer to obtain the needed information.

A medium-sophistication implementation would be if a provider creates an email distribution list alerting of new SBOMs. In the latter example email is still utilized; however, consumers no longer need to manually inquire about new SBOMs. This process is not personalized and may distribute information that is not relevant to each individual member of the distribution list, in addition to not providing historical or past SBOMS.

### Manufacturer Usage Description

Another technology that could be used for the Discovery phase is the Manufacturer Usage Description (MUD) standard,[12] which outlines how a device can distribute a reference to an SBOM or the SBOM itself, when it is connected to a network. This allows for the automated discovery of the associated SBOM for a system. However, this only provides direction to either a repository or a single SBOM; therefore, the MUD standard can be considered a medium-sophistication solution.

### Basic Web App

An example of a medium-sophistication implementation for a basic web app would be that the provider creates a static webpage containing the SBOM. For this example, a URL of the webpage would be distributed within reference documentation provided alongside a system, or the website would be attached to a well-known domain name.

### Feature Rich Web App

In a high-sophistication implementation example, a provider may create a subscription service that will list current and updated SBOMs. In this example, once a consumer is subscribed to the proper service, they do not need to take any additional manual action to become aware of updates or new SBOMs. In addition, it can be assumed the output of this subscription service is machine readable or otherwise sufficiently well-defined to enable automation.

### Distributed Ledger Synchronization

Like the subscription service noted in “Feature Rich Web App,” distributed ledger technologies may receive updates from peers about additional entries. This may occur as a series of transfers when a node is first initialized or it may occur frequently through peer-to-peer updates. This type of implementation would be described as a high-sophistication implementation due to the automatic propagation of updates.

## Access

After the location of an SBOM has been discovered, the next step is to obtain access to the data. This phase of the lifecycle focuses on access controls placed on the SBOM and how a consumer will gain authorization to continue to the Transport phase. There may be no requirements to have access controls in place and the SBOM will be available for public consumption. The provider may require that SBOMs be held in a repository that requires manual vetting to determine if access should be granted to an individual recipient. SBOMs may also require specific access control granularity ensuring consumers be allowed to view only specific versions of SBOMs associated with a product or access only specific portions of the information.

### *Access – Low Sophistication*

For low sophistication, the main attribute of the Access phase is the lack of authentication or access controls, or the highly manual nature of access controls. For any interface directly accessible to the consumer, it is assumed that the SBOMs are made public to all once they have been discovered. Another alternative is that access controls may be present, but they are determined manually on a case-by-case basis. For example, if a consumer requests an SBOM through email, then it would be up to the sender to determine whether a request should be fulfilled or not, and different individuals may answer or deny different types of requests. In addition, if the access controls are manual, there may be manually induced delays in response to requests for access.

### *Access – Medium Sophistication*

Medium sophistication requires that authentication be in place, as well as some level of access controls. Access controls may be role based (e.g., writer, reader, admin), or channel based (e.g., private, broadcast, public); however, in medium sophistication, it is assumed that full granularity of individual permissions is not present as that requires a full breakdown of each individual operation along with the different levels of permissions in that context. It can be assumed that the process of requesting access is either a partially automated process (e.g., an individual can submit a request through a web portal with defined fields) or a well-defined manual process (approvals needed from X specific individuals, SBOMs listed by a well-defined identifier, etc.).

### *Access – High Sophistication*

In high sophistication, a consumer may request access to view an SBOM, and a limited account may be created automatically. Access to SBOMs may be automatically provided if a consumer can provide evidence that they have purchased a device or software relevant to the SBOM in question. A high degree of permissions granularity is present along with roles or organization-level access controls. Due to the necessity of evaluating and fully understanding the permissions of each permissioned activity, as well as tracking the information necessary to automatically validate customer purchases, the features represent high sophistication.

For high sophistication, a provider may be able to delegate authentication and access control requests to another organization using a system, such as Public Key Infrastructure delegation using certificate signing, to allow individuals under that organization to gain access up to the level of parent organization.

### *Access Solution Examples*

This section provides examples of how the various sophistication levels could be applied to different types of solutions regarding the Access phase.

#### *Email*

A low-sophistication implementation would be a provider manually vetting requests for an SBOM when responding to a consumer's emailed request.

#### *Basic Web App*

A medium implementation would be the use of a login portal with manual review of account creation requests. This is a medium-sophistication level example due to the partially manual, partially automated nature of the request process, as well as the implicit authentication requirement.

#### *Feature Rich Web App*

A high-sophistication implementation would be the use of a login portal with automation involved in the account creation process. In this example, it is assumed that whether a limited account with restricted access is created initially, a consumer must provide a serial number, purchase order number, etc. Consumers can obtain access in an automated fashion without major manual intervention.

Once the necessary permissions and access have been obtained by a consumer, the consumer will be able to read, download, or otherwise obtain the SBOM data itself. This is described by the following Transport phase of the SBOM sharing lifecycle.

## Transport

The Transport Lifecycle phase denotes how a consumer receives the SBOM. Methods of transport may enable SBOMs to be transferred from single point to single point, or a single point to multiple points. Different methods facilitate this process more effectively than others. If the SBOM transport only involves the movement of a single SBOM, then an email or copy placed on a hard drive and sent from the author to the consumer may be sufficient. If there is a broad consumer base that requires the SBOM, then a method should be available that allows consumers to securely retrieve the SBOM. This phase is essential to enable the consumer to utilize the data.

### *Transport – Low Sophistication*

A low-sophistication transport process could involve the provider manually sending an SBOM to anyone who requests it. For example, the provider sends the SBOM as an email attachment. Within low transport, this movement of data is predominantly point-to-point in nature as sending to multiple consumers requires gathering of all consumers who need an SBOM. Another tendency of low sophistication is that data is "pushed" by the provider as opposed to "pulled" by the consumer.

Low sophistication does not also mandate transport over the Internet. For example, if an SBOM is verbally described or provided through the postal system, then this too would be a low-sophistication solution.

### *Transport – Medium Sophistication*

For medium sophistication, the Transport phase can be done using well-known methods like download through HTTP(S); however, documentation that supports this transport may still be minimal, and interfaces may be inconsistent or limiting, increasing the cost and expertise of automating the transport process to a high degree.

### *Transport – High Sophistication*

For high sophistication, the Transport phase process should be well documented using standard protocols. An application programming interface (API) should be present, consistent, and repeatable. An OpenAPI interface that provides documentation for a Representational State Transfer (REST) or RESTful API would be sufficient to be categorized at a high-sophistication level.[13] Although REST is a popular example of a standardized interface, other API standards, such as Simple Object Access Protocol (SOAP) or Graph Query Language (GraphQL), are also well-known and defined. Indeed, any interfaces that provide a similar ease of integration are also sufficient to be placed in the high-sophistication level. One such example of a further abroad transport mechanism would be the various synchronization protocols used by distributed ledgers to push and retrieve updates to the ledger.

### *Transport Solution Examples*

For the Transport phase, several examples are provided for how the sophistication level could be evaluated.

#### *Email*

A low-sophistication implementation would be the manual generation of a single email per requestor in which the desired SBOM would be attached.

#### *Basic Web App*

A medium implementation would be the creation of a website that allows for programmatic retrieval of data through scripts, although there are no dedicated API endpoints. There is potentially non-standardized formatting and an automated approach that may have to deal with non-standard responses or inconsistent data.

#### *Feature Rich Web App*

A high implementation would be the creation of a website that provides documented APIs to consumers. In this example, it is assumed that the API is described by well-known or otherwise largely descriptive documentation, which informs the consumer of exactly what operations they need to make to download or read an SBOM, as well as the expected response.

This implementation allows a consumer to construct their own process to obtain SBOMs according to their needs.

#### *Publish and Subscribe*

An implementation of the publish and subscribe pattern would be an example of a high-sophistication transport system. Within a publish and subscribe (pub/sub) system, one or more “publishers” generate and publish content, which is then automatically distributed to “subscribers” who subscribe to channels or groups of content based on their interests. In this system once a “subscriber”

subscribes to a given channel (i.e., one which contains the information for a given product or device), no further action is necessary on their part to receive updates for the product in which they are interested.

### Enrichment

Enrichment describes how an SBOM may be used to create a new product, before or after it has been shared with an additional party. For example, the SBOM may be reviewed and updated,[14] thus creating a new SBOM that could be moved through another instance of the SBOM sharing lifecycle.

Outputs of this process may not be SBOMs at all. For example, if a third party receives an SBOM and analyzes it to determine what common vulnerabilities and exposures are applicable to the described software, then this too would be an output of this process. Additional documents, such as Vulnerability Exploitability eXchange (VEX), which may refer to a product that is described by an SBOM, are also defined as enrichment activities. Enrichment data may be moved using the same methods of transport for SBOM data.

With enrichment being in an early developmental stage, private companies have developed tools to assist with this process. Repositories with enrichment data attached to SBOMs have been created. Many of these services are using cloud-based or distributed ledger technologies. Further work will be needed to evaluate enrichment in the context of sophistication.

## SBOM SHARING SURVEY

### Survey Overview

To understand the current state of SBOM sharing among stakeholders, organizations were surveyed on how they shared SBOMs. To begin the survey, 39 organizations were emailed an invitation to discuss the details of how the organizations shared their SBOMs. This invitation elicited 21 responses and included organizations that create platforms with a variety of SBOM discovery, access, transport, and storage functionality. All respondents were either interviewed via video teleconference or responded to emailed questions, based upon their availability. The interviewer asked the interviewee for a narrative response for how the organization handles the sharing of SBOMs. With a response, the interview proceeded with follow-up questions until the interviewer had created a sufficient profile of the organization's SBOM transport abilities.

### Survey Results Categorization

Once surveys were completed, efforts were made to understand the results by classifying the responses into general categories. The NTIA's "Sharing and Exchanging SBOMs"[15] document includes insight on how current solutions may be categorized. The document highlights three methods of sharing SBOMs, but it is clear from the document that these three methods are not to be considered an exhaustive list of transfer mechanisms. The three transfer methods in the NTIA document are: (1) the SBOM is provided directly to the receiver through email or similar informal communication mechanisms that are determined by pre-arrangement between the SBOM supplier and downstream authors and end users; (2) the SBOM resides on the device or system executing the software described by the SBOM; and (3) the SBOM resides on a repository available to software consumers.

The three categories were chosen as the starting point for the survey result categorization because of NTIA's initial leadership role. No survey responses demonstrated use of SBOM sharing where the SBOM is resident on the device executing the software described by the SBOM Transport Method 2.[e] The results of the survey and examples of both Transport Methods 1 and 3 are included below.

## Transport Method 1: SBOM is Provided Directly to the Receiver Using Email or Similar "Out-of-Band" Mechanism

The least sophisticated out-of-band mechanism for SBOM sharing that was identified in the survey is a conversation between supplier and asset owner over whether the supplier's asset is impacted by a particular vulnerability. To understand whether the asset is impacted, the supplier must take the time to understand through dialogue which asset the owner possesses. This conversation, where the asset owner's exact product and its dependencies are deduced by the supplier, can provide what may be considered the sharing of a verbal SBOM. This person-to-person communication is arguably the least-efficient method currently used based on the amount of time both parties may expend in the process.

In addition to person-to-person communication, survey participants are using email to transport SBOMs to those who send requests. Access controls with varying sophistication levels may be present with the body or attachment of such emails encrypted as well as the connection to a given email server. Many of those currently using emails are not necessary viewing email as a terminal solution, but as a stop gap while additional SBOM transport solutions of varying sophistication are considered.

## Transport Method 3: SBOM Resides on a Repository Available to Software Consumers

Many survey participants responded with SBOM sharing solutions that centered around using either existing infrastructure or the infrastructure of a third party. Some respondent organizations posted SBOMs on their existing self-service support websites without user registration to be discovered and accessed while others responded that they are using more sophisticated existing customer web-based service portals, where customers may use a login to access and transport technical information, such as SBOMs. Other survey participants responded that they use remote accessible file systems (e.g., Dropbox, Box.com, Amazon Simple Storage Service [S3]) to leverage third-party infrastructure to transport SBOMs. This use of remote accessible file systems comes in the form of an HTTPS link sent in an email or other electronic message or the sharing of login access information to directly access and transport SBOMs.

As SBOMs become more ubiquitous, cloud-based platform products have emerged that allow consumers to store different artifacts and provide discovery, access, and transport features so that users can share SBOMs with entities of the users' choosing. Many of these platform products provide additional high-sophistication services, such as risk intelligence on software/firmware packages and their associated SBOMs. Survey participants who used different cloud-based platforms noted different ways to discover and access SBOMs, including direct website links and the use of a web portal

e Examples in NTIA's Sharing and Exchanging SBOMs of "Method 2: SBOM is resident on the device executing the software the SBOM describes" include protocols such as HTTP, Constrained Application Protocol (CoAP), or an OpenC2 binding.

account. These platforms have a variety of different features, including customer data subscriptions for access to data on an automated and continuous basis. Some of the cloud-based solutions are based upon more sophisticated technologies, such as blockchain and/or distributed ledgers, to support access and transporting SBOMs and other supply chain information. Additional transport solutions allow an SBOM owner to use open-source software nodes to discover, access, and transport SBOMs stored on chosen data repositories with other appropriate parties.

## CONCLUSIONS

Based on the findings of this report, the path to widespread sharing of SBOMs involves increasing capabilities that focus on automation and interoperability within the SBOM sharing lifecycle phases. One strategy to promote this is to find ways of lowering the costs associated with higher sophistication solutions. While some parties may use low-sophistication solutions because they meet their needs, there may be other parties who do not use higher sophistication solutions because they simply lack the time, resources, subject-matter expertise, effort, and access to tooling needed to implement a high-sophistication solution in a particular phase of the SBOM sharing lifecycle. For example, an open-source software party may not have the same business drivers as a closed-source software developer that would necessitate a high-sophistication solution in the Discovery, Access, or Transport phases.

The SBOM sharing ecosystem would benefit from a variety of sharing solutions created by parties seeking to meet stakeholders' unique circumstances. These circumstances exist because a given supplier may be asked for different transport mechanisms from their customers while a customer may be offered SBOM data via different mechanisms from their upstream partners. These solutions can address the identified unique circumstances while also attempting to remove manual processes when possible and steer away from practices that discourage interoperability. Given the reality that different SBOM sharing approaches continue to be developed, interoperability between existing and future solutions should be a priority to avoid the creation of a variety of SBOM sharing solutions that cannot cooperate in the larger supply chain.

## FUTURE WORK

This document introduces a framework for evaluating different solutions for SBOM Discovery, Access, and Transport phases, as well as provides the reader with better understanding of the current SBOM sharing landscape. Because advances in sharing are critical to SBOM adoption, additional work on SBOM sharing will need to be completed soon. Indeed, industry has already begun to create private sharing solutions and services in addition to other ongoing efforts.[16,17] In particular, the concept of SBOM enrichment should be explored to understand the different activities and products that may constitute enrichment. Additional necessary work may also include a broader SBOM survey to better understand the SBOM user base and a review of the included desirable features with an eye toward maturing the exchange framework and providing users with recommended features.

# REFERENCES


1 NTIA (2018) “NTIA Launches Initiative to Improve Software Component Transparency,” National Telecommunications and Information Administration, https://ntia.doc.gov/blog/ntia-launches-initiative-improve-software-component-transparency.

2 CISA, “CISA SBOM-a-rama,” Cybersecurity & Infrastructure Security Agency, December 15–16, 2023, https://www.cisa.gov/resources-tools/resources/cisa-sbom-rama

3 Federal Register (2022) Public Listening Sessions on Advancing SBOM Technology, Processes, and Practices,” National Archives and Records Administration, June 2022, https://www.federalregister.gov/documents/2022/06/01/2022-11733/public-listening-sessions-on-advancing-sbom-technology-processes-and-practices.

4 NTIA (2021) “Sharing and Exchanging SBOMs,” National Telecommunications and Information Administration, February 2021, https://ntia.gov/files/ntia/publications/ntia_sbom_sharing_exchanging_sboms-10feb2021.pdf.

5 NTIA (2023) “Software Bill of Materials,” National Telecommunications and Information Administration, https://ntia.gov/page/software-bill-materials.

6 CISA (2023) “Software Bill of Materials,” Cybersecurity and Infrastructure Security Agency, https://www.cisa.gov/sbom.

7 NTIA (2021) “Sharing and Exchanging SBOMS,” National Telecommunications and Information Administration, February 2021, https://www.ntia.gov/files/ntia/publications/ntia_sbom_sharing_exchanging_sboms-10feb2021.pdf.

8 NTIA (2021) “SBOM Tool Classification Taxonomy,” National Telecommunications and Information Administration, March 2021, https://www.ntia.gov/files/ntia/publications/ntia_sbom_tooling_taxonomy-2021mar30.pdf.

9 NTIA (2021) “Sharing and Exchanging SBOMS,” National Telecommunications and Information Administration. February 2021, https://www.ntia.gov/files/ntia/publications/ntia_sbom_sharing_exchanging_sboms-10feb2021.pdf.

10 NTIA (2021) “Sharing and Exchanging SBOMS,” National Telecommunications and Information Administration, February 2021, https://www.ntia.gov/files/ntia/publications/ntia_sbom_sharing_exchanging_sboms-10feb2021.pdf.

11 NTIA (2021) “SBOM Options and Decision Points,” National Telecommunications and Information Administration, April 2021, https://www.ntia.gov/files/ntia/publications/sbom_options_and_decision_points_20210427-1.pdf.

12 IETF (2022) “Discovering and Retrieving Software Transparency and Vulnerability Information,” IETF Datatracker, September 2022, https://datatracker.ietf.org/doc/html/draft-ietf-opsawg-sbom-access-05#section-1.1.

13 OpenAPI (2021) “OpenAPI Specification V3.1.0,” OpenAPI, February 2021, https://spec.openapis.org/oas/latest.html.

14 NTIA (2021) “Survey of Existing SBOM Formats and Standards,” National Telecommunications and Information Administration, 2021, https://www.ntia.gov/files/ntia/publications/sbom_formats_survey-version-2021.pdf.

15 NTIA (2022) “Software Bill of Materials,” National Telecommunications and Information Administration, https://www.ntia.gov/files/ntia/publications/ntia_sbom_sharing_exchanging_sboms-10feb2021.pdf.

16 IETF (2022) “Supply Chain Integrity, Transparency, and Trust (scitt),” IETF Datatracker, 2022, https://datatracker.ietf.org/wg/scitt/about/.

17 Google (2022) “Announcing GUAC, a great pairing with SLSA (and SBOM)! Google Security Blog, October 20, 2022, https://security.googleblog.com/2022/10/announcing-guac-great-pairing-with-slsa.html.