A Hardware Bill of Materials (HBOM) Framework for Supply Chain Risk Management

Publication: September 2023
Cybersecurity and Infrastructure Security Agency

This page is intentionally left blank.

Contents

1. Introduction 1
1.1. The Benefits of Illuminating Upstream Supply Chain Risks and the Role of HBOMs 1
1.2. Recommendations for Use 2
1.3. Scope 2
2. User Manual and Documentation 3
Appendix A. .... HBOM Use Cases 4
A.1. Use Case Categories and Sub-Categories 4
A.2. HBOM Data Field Categories 5
A.3. Category Mapping 6
A.4. Examples 6
Appendix B. .... Format of HBOMs 8
B.1. HBOM Format Examples 8
B.2. Mapping to SBOM formats 10
Appendix C. .... HBOM Taxonomy 11
C.1. Field Category: HBOM Header Information 11
C.2. Field Category: Finished Good Product Details 12
C.3. Field Category: Entity Name 12
C.4. Field Category: Entity Location 13
C.5. Field Category: Component Part Information 17
C.6. Field Category: Component Part Details 18
C.7. Field Category: Production Details 19
C.8. Taxonomy Table – Quick Reference Guide 21
Appendix D. .... Potential Enhancements and Add-Ons to This Tool 26

Figures

Figure 1 — Example HBOM Break Down 8

Tables

Table 1 — Use Case Category Definitions 4
Table 2 — Use Case Sub-Category Definitions 4
Table 3 — HBOM Data Field Categories 5
Table 4 — HBOM Use Case to Data Field Mapping 6
Table 5 — HBOM Part Nesting Approach: Parent-Child 9
Table 6 — HBOM Product Manufacturing Details 9
Table 7 — HBOM Semiconductor Component Details 10

1. INTRODUCTION

The Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force[i] is a public-private, cross-sector body organized and co-chaired by the Cybersecurity and Infrastructure Security Agency (CISA), through a National Risk Management Center (NRMC) representative, and representatives from the Information Technology (IT) and Communications Critical Infrastructure Sectors. The Task Force serves as the primary mechanism for industry and government collaboration on strategies and policies to address ICT supply chain risks confronted by critical infrastructure owners and operators, civilian federal executive branch departments and agencies, and state, local, tribal, and territorial (SLTT) governments. The Task Force provides advice and recommendations to the federal government, and to private sector owners and operators of critical infrastructure on means for assessing and managing risks associated with the ICT supply chain.

The Task Force established the Hardware Bill of Materials (HBOM) Working Group (WG),[ii] which developed this Hardware Bill of Materials Framework to create a consistent, repeatable way for vendors to communicate with purchasers of hardware components in products that they have or may purchase. This will enable purchasers to evaluate and mitigate risks in their supply chain. The framework's objective is to set forth a reliable and predictable structure for HBOMs and a set of clearly defined data fields of HBOM components and their attributes, promoting efficiencies across the ICT sectors for a variety of use cases.

1.1. The Benefits of Illuminating Upstream Supply Chain Risks and the Role of HBOMs

The HBOM WG developed the HBOM Framework to provide a useful tool to help industry and government evaluate and address supply chain risks, especially those identified by past ICT SCRM Task Force reports. These past reports have identified multiple economic and security risks associated with equipment components that may be untrusted, compromised, or subject to availability risks. The same reports have described the benefits of developing tools to illuminate supply chains. For example:

- The Task Force's "Threat Scenarios Report" concluded that hardware components can introduce both economic risks, as well as security risks associated with untrusted or compromised components.[1]
- The Task Force's report on supply chain lessons learned from COVID-19 concluded that customers need more visibility into upstream supply chain constraints such as single-source or single-region "sub-tier" suppliers. It advised that the ICT industry may benefit from "development of standardized mapping and other illumination tools."[2]

In response to those conclusions, the HBOM WG developed an HBOM approach with a supporting tool that should help organizations illuminate supply chains and support the efficient evaluation and mitigation of some of those risks. As described in detail in this report, the HBOM WG considered the various use cases that providing HBOMs can address. For example, private sector entities need to be able to comply with applicable laws and regulations that prohibit purchases of equipment that contain components created by slave labor, which is an important use case for HBOMs.

[i] The Task Force operates under, and complies with the requirements of, the Critical Infrastructure Partnership Advisory Council (CIPAC) when engaged in activities generally covered by the Federal Advisory Committee Act.

[ii] In December 2018, the Department of Homeland Security established the ICT SCRM Task Force—a public-private partnership charged with identifying challenges and developing actionable solutions to enhance global ICT supply chain resilience. *See* https://www.cisa.gov/resources-tools/groups/ict-supply-chain-risk-management-task-force. The working group that produced this report consisted of and was co-chaired by representatives from each of the Task Force's three categories of stakeholders: government agencies, IT companies, and communications service providers.

1.2. Recommendations for Use

The HBOM Framework recommends requesting HBOMs as one of the many activities that purchasers should leverage to evaluate their supply chains. This framework is intended to inform organizations about such HBOMs. As this document describes, current HBOM formats need some assistance to be portable between suppliers and purchasers. This document aims to advance such portability. However, further work will be required to achieve the necessary maturity for true interoperability, such as broader ICT industry discussion and proof-of-concept testing. The HBOM WG expects that the ICT industry will continue to work this topic until HBOM interoperability can be specified by purchasers and complied with by suppliers through industry norms, specifications, and standards.

Purchasers may also need to undertake additional activities to evaluate their supply chain risks, such as sending vendors questionnaires about their cybersecurity practices,[iii] and requesting Software Bill of Materials (SBOM) information.[iv] Purchasers and vendors can use the HBOM Framework on a voluntary basis to facilitate the exchange of information.

1.3. Scope

This HBOM Framework includes a consistent naming methodology for attributes of components, a consistent format for identifying and providing information about the different types of components, and guidance of what HBOM information is appropriate depending on the purpose for which purchasers and vendors will be utilizing the HBOM.

This HBOM Framework is meant to be flexible and allow purchasers and vendors to tailor it to their specific circumstances or use cases. It is meant to capture the components' HBOM information to be included at the time of the sale or exchange of goods. Stakeholders may need to update the HBOM during the lifecycle of a project. Stakeholders are encouraged to explore ways to enhance this framework to ensure appropriate updating as discussed briefly in Appendix D of this report,[v] which discusses items out of scope for this framework. For example, it may be reasonable to get a new HBOM when the vendor changes the version of a product that they offer.

Also, out of scope for this HBOM Framework is SBOM information. It is important to recognize that SBOM information is a crucial component of the overall BOM information needed by purchasers to identify and evaluate their overall supply chain risks. Accordingly, this framework endeavors to ensure consistency with other frameworks that are becoming prominent approaches to providing SBOM, such as CycloneDX and SPDX. As discussed in Appendix D, the SCRM Task Force recommends that additional work be scoped for promoting a future state where this HBOM Framework can merge with emerging SBOM frameworks.

The HBOM Framework provides basic information about including the firmware associated with the products' components (i.e., the provider of the firmware), but stops short of proposing a framework for examining the provenance and other attributes of that firmware.

[iii] The ICT SCRM Task Force has published the Vendor Supply Chain Risk Management (SCRM) Template, which provides a set of questions regarding an ICT supplier's/provider's implementation and application of industry standards and best practices that can help guide supply chain risk planning in a standardized way. See https://www.cisa.gov/resources-tools/resources/ict-scrm-task-force-vendor-template.
[iv] There are a number of SBOM activities underway at CISA and elsewhere. For more information, please visit https://www.cisa.gov/sbom.
[v] See Appendix D, *Potential Enhancements and Add-Ons to This Tool*.

2. USER MANUAL AND DOCUMENTATION

As previously mentioned, the intent of this framework is for vendors and purchasers to use it on a voluntary and flexible basis; however, it can assist vendors and purchasers with determining the appropriate components to be included in the HBOM for a project in two important ways. First, it provides definitional and formatting consistency that is helpful regardless of the specific HBOM information being shared. Second, it provides guidance on what HBOM components may be appropriate to include in HBOMs that are provided to meet different use cases/goals that purchasers may have (e.g., evaluating security, promoting resiliency/availability, or complying with laws or regulations).

This HBOM Framework has several key components:

- **HBOM Use Case Categories (Appendix A):** Appendix A provides a range of potential use cases that purchasers may have for HBOMs based on the nature of the risk the purchaser seeks to evaluate. Because different use cases address different types of risk, each use case maps a different subset of data fields described above and in Appendix A.
- **Format of HBOMs (Appendix B)**: In Appendix B, the framework sets forth a format that can be used to ensure consistency across HBOMs and to increase the ease with which vendors and purchasers produce and use HBOMs. It includes a method for describing “nesting” of components where a vendor purchases an assembly from a third party, and that assembly requires further HBOM information to properly identify supply chain issues that are farther up in the supply chain.
- **Data Field Taxonomy (Appendix C):** Appendix C provides a taxonomy of component/input attributes that, depending on the use for which the purchaser intends to use an HBOM, may be appropriate to include in an HBOM. The taxonomy seeks to create consistency across HBOMs by defining a data field associated with each attribute. The specific set of data fields to be included in an HBOM may be informed by the recommendations below regarding which use cases require which types of information.

APPENDIX A - HBOM USE CASES

A.1. Use Case Categories and Sub-Categories

There are multiple reasons for a purchaser to request an HBOM from a vendor. These include: (1) identifying potential security risks associated with components in the product, (2) identifying the risk that the purchaser's supply chain may not be sufficiently diversified, and (3) ensuring compliance with government laws and regulations that may prohibit certain components. These assessments can be executed as part of a proactive exercise, audit requirements or a reactive evaluation. The principal HBOM use cases were identified by the ICT industry representative and government stakeholders as relevant for supply chain risk management purposes. These principal HBOM use cases can be categorized into three high-level categories, as described in Table 1.

TABLE 1: USE CASE CATEGORY DEFINITIONS

Use Case Category	Category Definition
Compliance	Situations which assess the product's compliance with rules and regulations. These scenarios will assess the adherence to internal, industry, and customer requirements.
Security	Scenarios that evaluate the product's security risk based on the exposure to known vulnerabilities and/or high susceptibility to untrusted entities/geolocations.
Availability	Conditions that assess product impacts from world events and supply chain diversification (or lack thereof).

Each of the high-level categories can be further broken down into sub-categories. The sub-category definitions and its hierarchy can be found in Table 2 below.

TABLE 2: USE CASE SUB-CATEGORY DEFINITIONS

Use Case Category	Use Case Sub-Category	Sub-Category Definition
Compliance	Government	Use Cases that involve compliance to government-related rules and regulations, such as Fiscal Year 2019 NDAA Sec. 889, UFLPA, WROs.
Compliance	Industry or Customer	Use Cases that involve compliance to industry-specific or customer-specific requirements (e.g., customer request for supply chain assessments).
Compliance	Internal and Quality	Use Cases that involve compliance to internal and product-specific requirements, policies, and procedures (e.g., procuring from only OEM-authorized vendors, adherence to PCNs).
Security	Geography and Entity Level	Use Cases that assess security risks involving untrusted/compromised entities, infrastructure, and concentrations at a macro level (i.e., geography or entity-level assessments).
Security	Product and Component Level	Use Cases that assess security risks involving untrusted, compromised, or counterfeit products and components (i.e., product or component level assessments).
Availability	World Events	Use Cases that assess the impact of world news events on the supply chain (e.g., the impact of

Use Case Category	Use Case Sub-Category	Sub-Category Definition
		COVID-19 on suppliers/manufacturers, the effect on lead time due to the railroad strike).
Availability	Clustering: Risks	Use Cases that assess the commonalities/single-points-of-failure and the probable impact on supply chain resiliency.
Availability	Clustering: Optimize	Use Cases that assess the commonalities with the intent to optimize and gain efficiencies.

Note: The individual use cases may fit multiple categories/sub-categories. To maintain a single classification per use case, the use case will be classified based on the hierarchy of Compliance, Security, and Availability as ordered in the table above.

A.2. HBOM Data Field Categories

The HBOM's individual data fields can be classified into high-level field categories. The field categories, and their respective details, can be found in Table 3 below. Additional detail of the data fields can be found in Appendix C.

TABLE 3: HBOM DATA FIELD CATEGORIES

Field Category	Definition	Example Data Fields
HBOM Header Information	Identifying information about the HBOM (Finished Good - Descriptive Information and HBOM Author/Dates)	Author, Create/Modify Dates, Product Type, Name, Description, Supplier/OEM
Entity Name	Company Names of Entities in the HBOM	(Contract) Manufacturer Name, Assembly & Test Supplier, Component Manufacturer/Supplier
Entity Location	Company Locations of Entities in the HBOM	Location Details of any Specified Entity
Finished Good Product Details	Finished Good: Technical Information	Product Version
Component Part Information	Component: Descriptive Information	Component Type, Category, Number, Description
Component Part Details	Component: Technical Information	Component Version, Tech Specs
Production Details	Production/Operational Information	% Sourced from Supplier, Lead Times, Quantity, Tech Node

A.3. Category Mapping

The individual use case sub-categories (Table 2) each evaluate a different type of risk. Therefore, each subcategory may require a different set of HBOM data fields to complete the assessment. Table 4 details the association of the required HBOM data fields to each Use Case sub-category.[vi]

TABLE 4: HBOM USE CASE TO DATA FIELD MAPPING

Field Category	Compliance			Security		Availability		
	Gov	Industry or Customer	Internal and Quality	Geography and Entity-Level	Products and Components	World Events	Clustering: Risks	Clustering: Optimize
HBOM Header Information	X	X	X	X	X	X	X	X
Entity Name	X	X	X	X	X	X	X	X
Entity Location	X	X		X		X	X	X
Finished Good Product Details	X	X	X	X	X			
Component Part Information	X	X	X	X	X	X	X	X
Component Part Details	X	X	X	X	X			
Production Details					X	X	X	X

A.4. Examples

EXAMPLE 1: COMPLIANCE/GOVERNMENT: ADHERENCE TO THE UYGHUR FORCED LABOR PREVENTION ACT (UFLPA)

U.S. Customs and Border Protection states that the UFLPA "…establishes a rebuttable presumption that the importation of any goods, wares, articles, and merchandise mined, produced, or manufactured wholly or in part in the Xinjiang Uyghur Autonomous Region of the People's Republic of China, or produced by certain entities, is prohibited by Section 307 of the Tariff Act of 1930 and that such goods, wares, articles, and merchandise are not entitled to entry to the United States."[vii, 3] For companies seeking to address the potential legal and operational impacts of the act, a product's traceability should be thoroughly understood. The term "wholly or in part" (within the UFLPA) states that any component or material of the product cannot be linked to Xinjiang. Therefore, it may not be enough to understand who the manufacturer is and where the manufacturer is located. Deeper transparency into the product's supply chain may be required.[viii]

[vi] While the Field Category to Use Case mapping is required, there is flexibility to identify the pertinent data fields within each Field Category. The individual data fields are detailed in Appendix A.

[vii] See the UFLPA, which also applies to Chinese goods made with forced labor outside the Xinjiang Uyghur Autonomous Region by Uyghurs, Tibetans, and members of "other persecuted groups." For more information about the UFLPA, please visit https://www.congress.gov/bill/117th-congress/house-bill/1155/text.

[viii] This example, and other examples in this section, are intended to highlight possible uses of HBOM to address these situations. No attempt is made here to provide legal advice and the reader is cautioned to seek qualified counsel to ensure compliance with any applicable law or regulation.

To obtain this information, purchasers and vendors may consider an HBOM detailing product and component level details. The "Entity Name" and "Entity Location" field details will provide the comparison data necessary to inform any determination as to whether a product is affected by such a law. If flagged, the "HBOM Header," "Finished Good Product Details," "Component Part Information," and "Component Part Details" are necessary to determine the product and component impacts.

EXAMPLE 2: AVAILABILITY/WORLD EVENTS: CHINA'S ZERO-COVID POLICY TEMPORARILY SHUTS DOWN NON-ESSENTIAL BUSINESSES IN SHENZHEN

To determine the impact of this shutdown, the "Entity Location" field would be queried for any entities located in Shenzhen, China. A list of flagged products can be compiled from the "HBOM Header," "Finished Good Product Details," and "Component Part Information." The "Product Details" would be used to determine the impact on product availability and any potential contingency plans.

EXAMPLE 3: SECURITY/GEOGRAPHY AND ENTITY LEVEL: SUPPLIER COUNTRY OF ORIGIN OR SUPPLIER ENTITY RESTRICTED BY U.S. FEDERAL SECURITY REGULATIONS

In response to evolving security concerns, U.S. federal regulations are updated with listings of countries of origin or supplier entities that are restricted from entry into the United States or from use in certain applications. To investigate compliance with such regulations, the use of an HBOM may be helpful when conducting a review of a supplier's country of origin, therefore "HBOM Header Information," "Entity Name," "Entity Location," "Finished Good Product Details," "Component Part Information," and "Component Part Details" are required.[ix] Note that restricted content may be related to the finished good, one or more component(s), or handling of the product by a restricted entity or in a restricted geography.

Acknowledging that these regulations are periodically updated, an attestation of compliance from a supplier is not helpful except for a specific point in time. The HBOM remains applicable and useful when restricted content listings are amended.

[ix] The use of the HBOM Framework does not mean that a company has complied with any U.S. regulations or that a regulatory agency will automatically accept the HBOM framework as evidence of compliance with U.S. restrictions imposed by a security regulation.

APPENDIX B - FORMAT OF HBOMs

HBOM information is recommended for any product/kit/assembly that can be broken down into lesser components. When arranged in order of assembly level, this breakdown is sometimes referred to as a “hierarchical” bill of materials.

In the example below, “Assembly X1,” “Kit X2,” and “Assembly W2” can be separated into additional pieces. Depending on the use-case, key information may reside within these components and may be hidden at the assembly/kit level. For these scenarios, ensure that the level of granularity within the HBOM is sufficient.

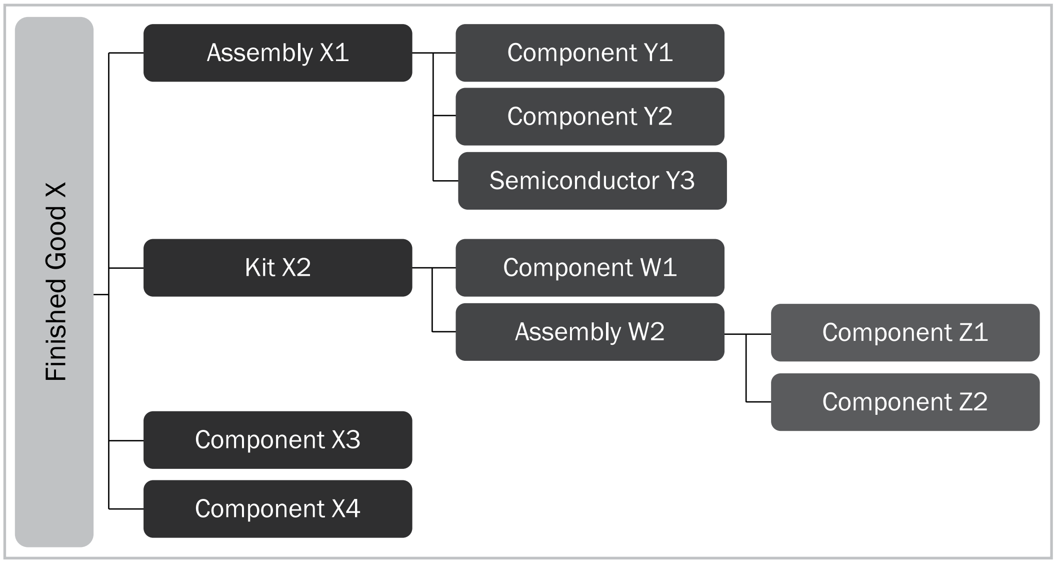

FIGURE 1: EXAMPLE HBOM BREAK DOWN

B.1. HBOM Format Examples

B.1.1. EXAMPLE: PARENT-CHILD NESTING (HIERARCHICAL)

This approach is suggested for spreadsheet HBOMs. An HBOM is recommended for any product/kit/assembly (parents) that be broken down into lesser components (children). For example, if assemblies are used in the production of the finished good, a separate HBOM is required for the assembly. The subsequent HBOMs can be nested together and joined via the part-level information. Table 5 below illustrates the four HBOMs for Finished Good X.

TABLE 5: HBOM PART NESTING APPROACH: PARENT-CHILD

General Information	Parent-Level Information: Finished Good/Kit/Assembly	Child-Level Information: Component/Semiconductor
HBOM 1	Finished Good X	Assembly X1
		Kit X2
		Component X3
		Component X4
HBOM 2	Assembly X1	Component Y1
		Component Y2
		Semiconductor Y3
HBOM 3	Kit X2	Component W1
		Assembly W2
HBOM 4	Assembly W2	Component Z1
		Component Z2

The result is a multi-level view of the Finished Good's HBOM. It may be helpful to use a separate tab or sheet for each level of assembly, such as a main unit (first sheet) that references a processor module (second sheet).

B.1.2. EXAMPLE: PRODUCT ORIGINAL EQUIPMENT MANUFACTURER (OEM) AND MANUFACTURING DETAILS

When providing an HBOM, detail may be required on the OEM, the manufacturer, and their locations. For these cases, it may be necessary to distinguish between the entities and location types. The example below details two sample scenarios and their differences:

TABLE 6: HBOM PRODUCT MANUFACTURING DETAILS

Field Name	Example: Manufacturer: Contract Manufacturer (CM)	Example: Manufacturer: OEM
fga_supplier	OEM Name	OEM Name
fga_supplier_loc	OEM HQ Location	OEM HQ Location
fga_main_manufacturer	CM	OEM Name
fga_main_location	CM Factory Location	OEM Factory Location

B.1.3. EXAMPLE: SEMICONDUCTOR COMPONENTS

Fabrication details are recommended for semiconductors, especially if foundry services are used. For these cases, request the supplier/OEM and the Fab/Foundry details as separate data points. If needed, also list the Assembly and Test details and tech node.

TABLE 7: HBOM SEMICONDUCTOR COMPONENT DETAILS

Field Name	Example: Manufacturer: Semiconductor Foundry	Example: Manufacturer: Supplier/OEM
comp_supplier	ACMECOM	ACMEcom
comp_manufacturer	Semiconductor Foundry LTD, Fab 10	ACMEcom, Fab A
comp_mfg_location	Fab 10 Location	Fab A Location
assy_and_test_supplier	XYZ Inc.	XYZ Inc.
assy_and_test_location	XYZ Inc.: Assembly and Test Site location	XYZ Inc.: Assembly and Test Site location
technology_node	10 nm	180nm

B.2 Mapping to SBOM Formats

Where possible, the field definitions that follow include a direct 1:1 mapping to alternative BOM formats such as CycloneDX and SPDX. If mapped, equivalent fields are defined in Appendix C. However, not all fields can be mapped using this method.

SCENARIO: FIELD EXISTS IN THE ALTERNATIVE BOM FORMAT, NO DIRECT 1:1 MAPPING

If an alternative BOM format contains a field “Country of Origin,” it is not possible to map directly on a 1:1 basis to the multiple location fields identified below. Such mapping will be different on a case-by-case basis depending on the user. The developer of conversion tooling will need to make an informed decision on what the appropriate mapping is for that use case.

SCENARIO: FIELD DOES NOT EXIST IN THE ALTERNATIVE BOM FORMAT

Alternative BOM formats often allow for flexibility via user-defined fields. If no equivalent field exists, the developer should create a user-defined field to provide the information to the requestor. All taxonomy-related information from the user-defined fields needs to be clearly communicated between the developer and the requestor.

APPENDIX C - HBOM TAXONOMY

C.1. Field Category: HBOM Header Information

These fields express information about the HBOM document itself, such as when the HBOM file was created.

C.1.1. FIELD NAME: HBOM_STD_VERSION

Field type: string
Description: Must be "1.0," this string represents the version of this HBOM Taxonomy
Example: "0.9"
Equivalent CycloneDX field: None, do not map
Equivalent SPDX field: None, do not map
Use Case Mapping: Compliance: All Security: All Availability: All

C.1.2. FIELD NAME: HBOM_CREATION_DATE

Field type: string
Description: Date that the HBOM Author created the BOM or pulled this document together in YYYY-MM-DD format (ISO 8601 format)
Example: "2022-11-22"
Equivalent CycloneDX field: None
Equivalent SPDX field: None
Use Case Mapping: Compliance: All Security: All Availability: All

C.1.3. FIELD NAME: HBOM_MODIFY_DATE

Field type: string
Description: Most recent date that the HBOM was edited (assumes HBOM is allowed to be modified) in YYYY-MM-DD format (ISO 8601 format)
Example: "2022-11-22"
Equivalent CycloneDX field: metadata/timestamp
Equivalent SPDX field: (2.9) Created:
Use Case Mapping: Compliance: All Security: All Availability: All

C.1.4. FIELD NAME: HBOM_AUTHOR

Field type: string
Description: HBOM Author's Name
Example: "John Smith"
Equivalent CycloneDX field: metadata/authors/author
Equivalent SPDX field: (2.8) Creator:
Use Case Mapping: Compliance: All Security: All Availability: All

C.1.5. FIELD NAME: FGA_SUPPLIER

Field type: string
Description: Finished Good OEM for the subject of this HBOM
Example: "MakeCo"
Equivalent CycloneDX field: None

Equivalent SPDX field: None
Use Case Mapping: Compliance: All Security: All Availability: All

C.1.6. FIELD NAME: FGA_NUM

Field type: string
Description: Unique Number issued by manufacturer to identify the product that is the subject of this HBOM
Example: “543245326”
Equivalent CycloneDX field: name
Equivalent SPDX field: (3.1) PackageName:
Use Case Mapping: Compliance: All Security: All Availability: All

C.1.7. FIELD NAME: FGA_DESCRIPTION

Field type: string
Description: Description of the product that is the subject of this HBOM
Example: “SetTopBox - Rev 5”
Equivalent CycloneDX field: None
Equivalent SPDX field: None
Use Case Mapping: Compliance: All Security: All Availability: All

C.2. Field Category: Finished Good Product Details

C.2.1. FIELD NAME: FGA_TYPE

Field type: enum (string) {“hardware” | “software” | “service” | *}
Description: Choose one of the following for the subject of this HBOM: “Hardware,” “Software,” “Service;” another string may be used but if possible the predefined values here should be used.
Example: “Hardware”
Equivalent CycloneDX field: None
Equivalent SPDX field: None
Use Case Mapping: Compliance: All Security: All Availability: All

C.2.2. FIELD NAME: FGA_VERSION

Field type: string
Description: Hardware, and/or Software, and/or Firmware version number, as shipped from the supplier
Example: “Hardware Version 3.2”; or “Firmware Version 13.3.3.2”
Equivalent CycloneDX field: version
Equivalent SPDX field: (3.3) PackageVersion:
Use Case Mapping: Compliance: All Security: All Availability: ---

C.3. Field Category: Entity Name

C.3.1. FIELD NAME: FGA_HASH

Field type: string
Description: An intrinsic identifier for the subject of this HBOM; if this is a top-level HBOM it is an identifier for the FGA. Otherwise, it is an identifier for a component such as a system on a chip (SoC).
Example: “A999999A-D999-4DD4-A640-98B76543A210”

Equivalent CycloneDX field: Hash “alg”
Equivalent SPDX field: (3.10) PackageChecksum: (3.9) PackageVerificationCode:
Use Case Mapping: Compliance: All Security: All Availability: --

C.3.2. FIELD NAME: FGA_MAIN_MANUFACTURER

Field type: string
Description: Company those manufacturers or assembles the product (if the OEM uses a Contract Manufacturer, list the Contract Manufacturer here. If the OEM is the manufacturer, list the OEM.)
Example: “STB Manufacturing, Inc”
Equivalent CycloneDX field: Supplier publisher
Equivalent SPDX field: (3.5) PackageSupplier:
Use Case Mapping: Compliance: All Security: All Availability: All

C.3.3. FIELD NAME: FGA_ALT_MANUFACTURER

Field type: string
Description: Alternate company that manufacturers or assembles the product, if the primary location is incapacitated
Example: “Home Devices, LLC”
Equivalent CycloneDX field: None
Equivalent SPDX field: None
Use Case Mapping: Compliance: All Security: All Availability: All

C.3.4. FIELD NAME: COMP_SUPPLIER

Field type: string
Description: Component Supplier (if not purchased directly from OEM)
Example: “Component World”
Equivalent CycloneDX field: None
Equivalent SPDX field: None
Use Case Mapping: Compliance: All Security: All Availability: All

C.3.5. FIELD NAME: COMP_MANUFACTURER

Field type: string
Description: Component Manufacturer (If Semiconductor, list the Fab name as well)
Example: “SanCap LLC”
Equivalent CycloneDX field: Supplier publisher
Equivalent SPDX field: (3.5) PackageSupplier:
Use Case Mapping: Compliance: All Security: All Availability: All

C.4. Field Category: Entity Location

C.4.1. FIELD NAME: ASSY_AND_TEST_SUPPLIER

Field type: string
Description: For Semiconductor parts only: provide the Assembly and Test (A&T) Supplier
Example: “SanCap Assembly and Test”
Equivalent CycloneDX field: None
Equivalent SPDX field: None
Use Case Mapping: Compliance: All Security: All Availability: All

C.4.2. FIELD NAME: FGA_SUPPLIER_LOC

Field type: string
Description: Finished Good Product: OEM Headquarter location
Example: “New York, New York, United States”
Equivalent CycloneDX field: None
Equivalent SPDX field: None
Use Case Mapping: Compliance: Government, Industry/Customer Security: Geography/Entity-Level Availability: All
Similar/Substitutable Fields: OEM Location: Option 1 of 3

C.4.3. FIELD NAME: FGA_LOC_COORDS

Field type: string
Description: Latitude and longitude coordinates of the OEM's headquarter location in Decimal Degree format
Example: “40.7128, -74.0060”
Equivalent CycloneDX field: None
Equivalent SPDX field: None
Use Case Mapping: Compliance: Government, Industry/Customer Security: Geography/Entity-Level Availability: All
Similar/Substitutable Fields: OEM Location: Option 2 of 3

C.4.4. FIELD NAME: FGA_LOC_CODE

Field type: string
Description: OEM Headquarter location in ISO Standard for Country and Subdivisions. Example: “US-MA”: Country: USA, State: Massachusetts
Example: “US-NY”
Equivalent CycloneDX field: None
Equivalent SPDX field: None
Use Case Mapping: Compliance: Government, Industry/Customer Security: Geography/Entity-Level Availability: All
Similar/Substitutable Fields: OEM Location: Option 3 of 3

C.4.5. FIELD NAME: FGA_MAIN_LOCATION

Field type: string
Description: Location(s) where product was assembled or manufactured
Example: “Chengdou, Fujian, China “
Equivalent CycloneDX field: None
Equivalent SPDX field: None
Use Case Mapping: Compliance: Government, Industry/Customer Security: Geography/Entity-Level Availability: All
Similar/Substitutable Fields: Primary Manufacturing (MFG) Location: Option 1 of 3

C.4.6. FIELD NAME: FGA_MAIN_LOC_COORDS

Field type: string
Description: Latitude and longitude coordinates of the secondary MFG location in Decimal Degree format (WGS84)
Example: “27.2854, 120.3124”

Equivalent CycloneDX field: None
Equivalent SPDX field: None
Use Case Mapping: Compliance: Government, Industry/Customer Security: Geography/Entity-Level
Availability: All
Similar/Substitutable Fields: Primary MFG Location: Option 2 of 3

C.4.7. FIELD NAME: FGA_MAIN_LOC_CODE

Field type: string
Description: ISO Standard for Country and Subdivisions. Example: US-MA (Country is USA, State is Massachusetts)
Example: "CN-FJ"
Equivalent CycloneDX field: None
Equivalent SPDX field: None
Use Case Mapping: Compliance: Government, Industry/Customer Security: Geography/Entity-Level
Availability: All
Similar/Substitutable Fields: Primary MFG Location: Option 3 of 3

C.4.8. FIELD NAME: FGA_ALT_LOCATION

Field type: string
Description: Secondary/Alternate location(s) for product assembly or manufacturing
Example: "Austin, Texas, USA"
Equivalent CycloneDX field: None
Equivalent SPDX field: None
Use Case Mapping: Compliance: Government, Industry/Customer Security: Geography/Entity-Level
Availability: All

C.4.9. FIELD NAME: FGA_ALT_LOC_COORDS

Field type: string
Description: Latitude and longitude coordinates of the secondary MFG location in Decimal Degree format (WGS84)
Example: "30.2672, -97.7431"
Equivalent CycloneDX field: None
Equivalent SPDX field: None
Use Case Mapping: Compliance: Government, Industry/Customer Security: Geography/Entity-Level
Availability: All

C.4.10. FIELD NAME: FGA_ALT_LOC_CODE

Field type: string
Description: ISO Standard for Country and Subdivisions. Example: US-MA (Country is USA, State is Massachusetts)
Example: "US-TX"
Equivalent CycloneDX field: None
Equivalent SPDX field: None
Use Case Mapping: Compliance: Government, Industry/Customer Security: Geography/Entity-Level
Availability: All

C.4.11. FIELD NAME: COMP_MFG_LOCATION

Field type: string
Description: Manufacturing location of the component
Example: “Franklin, MA, USA”
Equivalent CycloneDX field: None
Equivalent SPDX field: None
Use Case Mapping: Compliance: Government, Industry/Customer Security: Geography/Entity-Level Availability: All
Similar/Substitutable Fields: Component MFG Location: Option 1 of 3

C.4.12. FIELD NAME: COMP_MFG_LOC_COORDS

Field type: string
Description: Latitude and longitude coordinates of the component MFG location in Decimal Degree format
Example: “42.0834, -71.3967”
Equivalent CycloneDX field: None
Equivalent SPDX field: None
Use Case Mapping: Compliance: Government, Industry/Customer Security: Geography/Entity-Level Availability: All
Similar/Substitutable Fields: Component MFG Location: Option 2 of 3

C.4.13. FIELD NAME: COMP_MFG_LOC_CODE

Field type: string
Description: ISO Standard for Country and Subdivisions. Example: “US-MA”: Country: USA, State: Massachusetts
Example: “US-MA”
Equivalent CycloneDX field: None
Equivalent SPDX field: None
Use Case Mapping: Compliance: Government, Industry/Customer Security: Geography/Entity-Level Availability: All
Similar/Substitutable Fields: Component MFG Location: Option 3 of 3

C.4.14. FIELD NAME: ASSY_AND_TEST_LOCATION

Field type: string
Description: For Semiconductor parts only: provide the Assembly&Test Location(s)
Example: “Franklin, MA, USA”
Equivalent CycloneDX field: None
Equivalent SPDX field: None
Use Case Mapping: Compliance: Government, Industry/Customer Security: Geography/Entity-Level Availability: All
Similar/Substitutable Fields: Component A&T Location: Option 1 of 3

C.4.15. FIELD NAME: ASSY_AND_TEST_LOC_COORDS

Field type: string
Description: For Semiconductor parts only: Latitude and longitude coordinates of the component Assembly and Test location in Decimal Degree format
Example: “42.0834, -71.3967”

Equivalent CycloneDX field: None
Equivalent SPDX field: None
Use Case Mapping: Compliance: Government, Industry/Customer Security: Geography/Entity-Level Availability: All
Similar/Substitutable Fields: Component A&T Location: Option 2 of 3

C.5. Field Category: Component Part Information

C.5.1. FIELD NAME: ASSY_AND_TEST_LOC_CODE

Field type: string
Description: For Semiconductor parts only: ISO Standard for Country and Subdivisions. Example: "US-MA": Country: USA, State: Massachusetts
Example: "US-MA"
Equivalent CycloneDX field: None
Equivalent SPDX field: None
Use Case Mapping: Compliance: Government, Industry/Customer Security: Geography/Entity-Level Availability: All
Similar/Substitutable Fields: Component assembly and test (A&T) Location: Option 3 of 3

C.5.2. FIELD NAME: COMP_SUPPLIER_PN

Field type: string
Description: Component unique identifier (enterprise resource planning (ERP) part number)
Example: "576375634"
Equivalent CycloneDX field: None
Equivalent SPDX field: (2.5) SPDX Document Namespace (3.2) SPDXID:
Use Case Mapping: Compliance: All Security: All Availability: All

C.5.3. FIELD NAME: COMP_MANUFACTURER_PN

Field type: string
Description: OEM's Manufacturing Part Number
Example: "CZ10UF2020"
Equivalent CycloneDX field: name
Equivalent SPDX field: (3.1) PackageName:
Use Case Mapping: Compliance: All Security: All Availability: All

C.5.4. FIELD NAME: COMP_DESCRIPTION

Field type: string
Description: Description of the component
Example: "10UF 10V-DC CAPACITOR"
Equivalent CycloneDX field: None
Equivalent SPDX field: None
Use Case Mapping: Compliance: All Security: All Availability: All

C.5.5. FIELD NAME: COMP_TYPE

Field type: enum (string) {"hardware" | "software" | "service" | *}
Description: Choose one of the following: "Hardware," "Software," "Service;" another string may be used but if possible the predefined values here should be used.

Example: “Hardware”
Equivalent CycloneDX field: None
Equivalent SPDX field: None
Use Case Mapping: Compliance: All Security: All Availability: All

C.5.6. FIELD NAME: COMP_PART_TYPE

Field type: string (* might enum this)
Description: Component category (e.g., semiconductor, antenna, etc.)
Example: “Capacitor”
Equivalent CycloneDX field: None
Equivalent SPDX field: None
Use Case Mapping: Compliance: All Security: All Availability: All

C.5.7. FIELD NAME: COMP_PART_CODE

Field type: string
Description: Industry-standard component code (e.g., surface mounted device (SMD)) capacitor codes)
Example: “ECA-0105Y-K31”
Equivalent CycloneDX field: None
Equivalent SPDX field: None
Use Case Mapping: Compliance: All Security: All Availability: All

C.5.8. FIELD NAME: COMP_HASH

Field type: string
Description: An intrinsic identifier for the component
Example: “A999999A-D999-4DD4-A640-98B76543A210”
Equivalent CycloneDX field: Hash “alg”
Equivalent SPDX field: (3.10) PackageChecksum: (3.9) PackageVerificationCode:
Use Case Mapping: Compliance: All Security: All Availability: All

C.6. Field Category: Component Part Details

C.6.1. FIELD NAME: COMP_OPT_NAME

Field type: string
Description: Optional, may be industry-standard or specific to a particular project
Example: “Mars Project Interface Adapter” (where “Mars Project” has meaning to the program but is not industry-recognized)
Equivalent CycloneDX field: None
Equivalent SPDX field: None
Use Case Mapping: Compliance: All Security: All Availability: All

C.6.2. FIELD NAME: COMP_VERSION

Field type: string
Description: Hardware, and/or Software, and/or Firmware version number, as shipped from the supplier
Example: “Hardware Version 3.2”; or “Firmware Version 13.3.3.2”
Equivalent CycloneDX field: version

Equivalent SPDX field: (3.3) PackageVersion:
Use Case Mapping: Compliance: All Security: All Availability: ---

C.7. Field Category: Production Details

C.7.1. FIELD NAME: COMP_DATASHEET

Field type: string
Description: Datasheet (published specifications or features as URI/URL)
Example: “https://www.CapacitorHouseUSA.com/ECA-0105Y/datasheet.pdf”
Equivalent CycloneDX field: None
Equivalent SPDX field: None
Use Case Mapping: Compliance: All Security: All Availability: ---

C.7.2. FIELD NAME: SUPPLIER_SOURCED_PCTG

Field type: float
Description: If the component is multi-sourced, provide the % sourced from this supplier.
Example: 0.5
Equivalent CycloneDX field: None
Equivalent SPDX field: None
Use Case Mapping: Compliance: --- Security: --- Availability: All

C.7.3. FIELD NAME: LEADTIMES

Field type: Integer (int)
Description: Provide the supplier's lead time in days.
Example: 20
Equivalent CycloneDX field: None
Equivalent SPDX field: None
Use Case Mapping: Compliance: --- Security: --- Availability: All

C.7.4. FIELD NAME: QUANTITY

Field type: int
Description: Quantity needed to produce one unit
Example: 2
Equivalent CycloneDX field: None
Equivalent SPDX field: None
Use Case Mapping: Compliance: --- Security: --- Availability: All

C.7.5. FIELD NAME: TECHNOLOGY_NODE

Field type: string
Description: For Semiconductor parts only: provide the process node in nm.
Example: n/a
Equivalent CycloneDX field: None
Equivalent SPDX field: None
Use Case Mapping: Compliance: --- Security: --- Availability: All

C.7.6. FIELD NAME: COMP_PART_SIZE_VAL

Field type: string
Description: Component size in a metric relevant to the type of component such as: footprint in an industry standard (e.g., 0402, 1005), or length (e.g., cable), or weight (e.g., glue), etc.
Example: 4
Equivalent CycloneDX field: None
Equivalent SPDX field: None
Use Case Mapping: Compliance: --- Security: --- Availability: All

C.7.7. FIELD NAME: COMP_PART_SIZE_UNIT

Field type: string
Description: Unit of measure for Component Size
Example: “gm”
Equivalent CycloneDX field: None
Equivalent SPDX field: None
Use Case Mapping: Compliance: --- Security: --- Availability: All

C.7.8. FIELD NAME: COMP_DATECODE

Field type: string
Description: Component timestamp/lot date code/lot number
Example: “230208” (date code), “23017” (year and week-of-year)
Equivalent CycloneDX field: None
Equivalent SPDX field: None
Use Case Mapping: Compliance: --- Security: --- Availability: All

C.8. Taxonomy Table – Quick Reference Guide

Field Category	Field Name	Description	Use Case Mapping
HBOM Header Information	hbom_std_version	Must be "1.0," this string represents the version of this HBOM Taxonomy	Compliance: All Security: All Availability: All
	hbom_creation_date	Date that the HBOM Author created the BOM or pulled this document together in YYYY-MM-DD format (ISO 8601 format)	Compliance: All Security: All Availability: All
	hbom_modify_date	Most recent date that the HBOM was edited (assumes HBOM is allowed to be modified) in YYYY-MM-DD format (ISO 8601 format)	Compliance: All Security: All Availability: All
	hbom_author	HBOM Author's Name	Compliance: All Security: All Availability: All
	fga_supplier	Finished Good OEM for the subject of this HBOM	Compliance: All Security: All Availability: All
	fga_num	Unique Number issued by manufacturer to identify the product that is the subject of this HBOM	Compliance: All Security: All Availability: All
	fga_description	Description of the product that is the subject of this HBOM	Compliance: All Security: All Availability: All
	fga_type	Choose one of the following for the subject of this HBOM: "Hardware," "Software," "Service;" another string may be used but, if possible, the predefined values here should be used	Compliance: All Security: All Availability: All
Finished Good Product Details	fga_version	Hardware, and/or Software, and/or Firmware version number, as shipped from the supplier	Compliance: All Security: All Availability: ---
	fga_hash	An intrinsic identifier for the subject of this HBOM; if this is a top-level HBOM it is an identifier for the FGA. Otherwise, it is an identifier for a component such as a SoC	Compliance: All Security: All Availability: ---

Field Category	Field Name	Description	Use Case Mapping
Entity Name	fga_main_manufacturer	Company that manufactures or assembles the product (If the OEM uses a Contract Manufacturer, list the Contract Manufacturer here. If the OEM is the manufacturer, list the OEM.)	Compliance: All Security: All Availability: All
	fga_alt_manufacturer	Alternate company that manufacturers or assembles the product if the primary location is incapacitated	Compliance: All Security: All Availability: All
	comp_supplier	Component Supplier (if not purchased directly from OEM)	Compliance: All Security: All Availability: All
	comp_manufacturer	Component Manufacturer (if Semiconductor, list the Fab name as well)	Compliance: All Security: All Availability: All
	assy_and_test_supplier	For Semiconductor parts only: provide the Assembly&Test Supplier	Compliance: All Security: All Availability: All
Entity Location	fga_supplier_loc	Finished Good Product: OEM Headquarter location	Compliance: Government, Industry/Customer Security: Geography/Entity-Level Availability: All
	fga_loc_coords	Latitude and longitude coordinates of the OEM's headquarter location in Decimal Degree format	Compliance: Government, Industry/Customer Security: Geography/Entity-Level Availability: All
	fga_loc_code	OEM Headquarter location in ISO Standard for Country and Subdivisions. Example: "US-MA": Country: USA, State: Massachusetts	Compliance: Government, Industry/Customer Security: Geography/Entity-Level Availability: All
	fga_main_location	Location(s) where product was assembled or manufactured	Compliance: Government, Industry/Customer Security: Geography/Entity-Level Availability: All
	fga_main_loc_coords	Latitude and longitude coordinates of the secondary MFG location in Decimal Degree format (WGS84)	Compliance: Government, Industry/Customer Security: Geography/Entity-Level Availability: All

Field Category	Field Name	Description	Use Case Mapping
	fga_main_loc_code	ISO Standard for Country and Subdivisions. Example: US-MA (Country is USA, State is Massachusetts)	Compliance: Government, Industry/Customer Security: Geography/Entity-Level Availability: All
	fga_alt_location	Secondary/Alternate location(s) for product assembly or manufacturing	Compliance: Government, Industry/Customer Security: Geography/Entity-Level Availability: All
	fga_alt_loc_coords	Latitude and longitude coordinates of the secondary MFG location in Decimal Degree format (WGS84)	Compliance: Government, Industry/Customer Security: Geography/Entity-Level Availability: All
	fga_alt_loc_code	ISO Standard for Country and Subdivisions. Example: US-MA (Country is USA, State is Massachusetts)	Compliance: Government, Industry/Customer Security: Geography/Entity-Level Availability: All
	comp_mfg_location	Manufacturing location of the component	Compliance: Government, Industry/Customer Security: Geography/Entity-Level Availability: All
	comp_mfg_loc_coords	Latitude and longitude coordinates of the component MFG location in Decimal Degree format	Compliance: Government, Industry/Customer Security: Geography/Entity-Level Availability: All
	comp_mfg_loc_code	ISO Standard for Country and Subdivisions. Example: "US-MA": Country: USA, State: Massachusetts	Compliance: Government, Industry/Customer Security: Geography/Entity-Level Availability: All
	assy_and_test_location	For Semiconductor parts only: provide the Assembly&Test Location(s)	Compliance: Government, Industry/Customer Security: Geography/Entity-Level Availability: All

Field Category	Field Name	Description	Use Case Mapping
	assy_and_test_loc_coords	For Semiconductor parts only: Latitude and longitude coordinates of the component Assembly and Test location in Decimal Degree format	Compliance: Government, Industry/Customer Security: Geography/Entity-Level Availability: All
	assy_and_test_loc_code	For Semiconductor parts only: ISO Standard for Country and Subdivisions. Example: "US-MA": Country: USA, State: Massachusetts	Compliance: Government, Industry/Customer Security: Geography/Entity-Level Availability: All
Component Part Information	comp_supplier_pn	Component unique identifier (ERP part number)	Compliance: All Security: All Availability: All
	comp_manufacturer_pn	OEM's Manufacturing Part Number	Compliance: All Security: All Availability: All
	comp_description	Description of the component	Compliance: All Security: All Availability: All
	comp_type	Choose one of the following: Hardware, Software, Service; another string may be used but, if possible, the predefined values here should be used	Compliance: All Security: All Availability: All
	comp_part_type	Component category (e.g., semiconductor, antenna, etc.)	Compliance: All Security: All Availability: All
	comp_part_code	Industry-standard component code (e.g., SMD capacitor codes)	Compliance: All Security: All Availability: All
	comp_hash	An intrinsic identifier for the component	Compliance: All Security: All Availability: All
	comp_opt_name	Optional, may be industry-standard or specific to a particular project	Compliance: All Security: All Availability: All
Component Part Details	comp_version	Hardware, and/or Software, and/or Firmware version number, as shipped from the supplier	Compliance: All Security: All Availability: ---
	comp_datasheet	Datasheet (published specifications or features as URI/URL)	Compliance: All Security: All Availability: ---
Production Details	supplier_sourced_pctg	If the component is multi-sourced, provide the % sourced from this supplier	Compliance: --- Security: --- Availability: All

Field Category	Field Name	Description	Use Case Mapping
	lead_times	Provide the supplier's lead time, in days	Compliance: --- Security: --- Availability: All
	quantity	Quantity needed to produce one unit	Compliance: --- Security: --- Availability: All
	technology_node	For Semiconductor parts only: provide the process node in nm	Compliance: --- Security: --- Availability: All
	comp_part_size_val	Component size in a metric relevant to the type of component such as: footprint in an industry standard (e.g., 0402, 1005), or length (e.g., cable), or weight (e.g., glue), etc.	Compliance: --- Security: --- Availability: All
	comp_part_size_unit	Unit of measure for Component Size	Compliance: --- Security: --- Availability: All
	comp_datecode	Component timestamp/lot date code/lot number	Compliance: --- Security: --- Availability: All

APPENDIX D - POTENTIAL ENHANCEMENTS AND ADD-ONS TO THIS TOOL

While the ICT SCRM Task Force HBOM WG is currently discussing out-of-scope topics, the following ideas could be considered:

First, future guidance is recommended to systematically address part and entity resolution challenges. Suppliers may provide HBOMs with nomenclature variations, and these variations and other disparities can hinder HBOM content evaluations and cause difficultly in linking a product's SBOM to its HBOM. As referenced in the National Telecommunications and Information Administration's (NTIA) "Software Identification Challenges and Guidance" document, one of the largest challenges of supply chain transparency and SBOMs is identifying software components with adequate distinctiveness.[4] The same challenge exists for HBOMs, where multiple identifiers can be used for the same part, and/or a generic identifier can be used to reference multiple parts.

- Example: Generic Identifier → Multiple Parts:
  - Apple iPhone 14 Plus → Various SKUs (different SKU per color and memory size)[x]
  - Samsung DDR4 64GB Memory → 21 different part numbers[xi]
- Example: Multiple Identifiers, Same Part
  - Qualcomm Snapdragon 888 = SM8350 part number[xii]
  - ACME RTZ-1234-LPIGE4453 = RTZ1234-LPIGE4453 = RTZ1234LPIGE4453

Entity names have a similar resolution problem, due to non-standard spelling, abbreviations, branding, etc. Various entity identification systems and standards exist—such as DUNS, SAM and CAGE; however, these systems are not fully inclusive, especially for small or foreign component manufacturers.

- Example: Multiple Entity Identifiers
  - Intel = Intel Corp = Intel Corporation
  - ASE = ASE Technology Holding Co = Advanced Semiconductor Engineering

Entity mergers, acquisitions, and corporate structures carry additional complexity. With mergers and acquisitions, part numbers, code names, and other identifiers may change due to rebranding. It is recommended to check for all possible permutations during the HBOM evaluation, as inventory and tracking systems may or may not link the parts/entities together, causing multiple instances to exist.

- Example: Cisco acquisition of Cerent → Multiple Identifiers due to rebranding
  - Cisco 800-06742-01 = Cerent 87-21-00002[xiii]

Additionally, it may be necessary to evaluate other organizations within an entity's corporate structure. For example, Fiscal Year 2019 NDAA Section 889 prohibits the government from obtaining video surveillance and telecommunications equipment from specific entities, such as Hytera Communications Corporation. These restrictions also span the entity's subsidiaries and affiliates.[xiv] For Hytera, this would include telecom equipment marketed and branded as PowerTrunk. Additional

[x] For more information about the Apple IPhone 14, please visit https://www.apple.com/shop/buy-iphone/iphone-14.
[xi] For more information about the Samsung DDR4 Semiconductor, please visit https://semiconductor.samsung.com/dram/module/.
[xii] For more information about the Qualcomm Snapdragon, please visit https://www.qualcomm.com/content/dam/qcomm-martech/dm-assets/documents/prod_brief_qcom_sd888_5g_0.pdf.
[xiii] For more information about Cisco ONS 15454 CLEI Codes, please visit https://www.cisco.com/c/en/us/support/docs/optical-networking/ons-15454-sonet-multiservice-provisioning-platform-mspp/46247-15454-cleicodes.html.
[xiv] For the complete NDAA Section 889 Prohibited Vendor List, please visit https://smartpay.gsa.gov/ndaa-section-889.

research may be needed to thoroughly check for restricted entity associations during HBOM evaluations.

This future guidance would provide recommended identification techniques and resources to address these complex part and entity resolution challenges. These challenges need to be overcome to accurately assess the HBOM and to pair the product with its appropriate SBOM for a complete evaluation.

1. Investigating what the techniques are for conveying and verifying the provenance, pedigree, and integrity of HBOMs. Similar discussions have occurred in the SBOM community activities, but the topic would have different aspects when addressing HBOMs.

2. A discussion about the roles involved in producing, gathering, publishing, sharing, and protecting HBOMs. The SBOM community has discussed and debated the different aspects of these topics for SBOMs, but there are probably slightly different concerns and needs that should be recognized when considering these for HBOMs.

3. Exploring the concept of operations for HBOMs. There are many open questions about how they would be used in operations. For example:

- Are HBOMs an internal capability for use within a supply chain so the parties in the supply chain can do their business more effectively, or are HBOMs a public aspect of a supply chain? Maybe some of both?
- Are HBOMs meant for humans or automation? If both, under what situations?
- What rights do customers of a supplier have for getting HBOMs?
- What contract clauses should one have to get HBOMs, if they aren't given freely?

4. Future work may be helpful to provide additional translation to alternative BOM formats. While some equivalent fields have been defined for CycloneDX and SPDX (as seen in Appendix C), at the current status, not all fields have a direct 1:1 mapping. In addition, not all BOM formats have been evaluated and mapped here. For example, Appendix C does not address mapping to the Catalog Data Standard being developed by the Department of Defense.[xv] Future guidance is recommended to further flesh this out so that HBOMs will be more interoperable and automated with minimum required conversion tooling and user-defined fields. Partnership with the CycloneDX, SPDX, and CDS knowledge base would be helpful to achieve these next steps.

[xv] For more information about the Department of Defense's Catalog Data Standard, please visit https://www.federalregister.gov/documents/2022/11/04/2022-24057/department-of-defense-catalog-data-standard.

HARDWARE BILL OF MATERIALS (HBOM) WORKING GROUP (WG) MEMBERS

Leadership team for HBOM WG:

	Name	Company
Co-Chair	Christopher Oatway	Verizon
Co-Chair	Thomas Gardner	HP
Co-Chair	Kanitra Tyler	NASA

HBOM WG consists of the following members:

Name	Company
Jeff Liang	Amazon
Alan Harrison, Chris Boyer, Rich Mosley	AT&T
Jeremy Bellay	Battelle
Justin Murphy	Cybersecurity and Infrastructure Security Agency (CISA)
Michael Bergman	Consumer Technology Association (CTA)
Laura Byrd, Mark Norman, Ronald Hertog	Dell
Jason Mullins, Mark Nguy	Department of Education
Cherylene Caddy, Drew Morin, Eric Tamarkin, Tim Vercruyssen	Department of Energy
Cedric Butts, John Schneider, Kuan Wang, Melanie McKinney, Michael Camp	Department of Defense (DoD)
Michele Iversen, Paul DeNaray	DoD CIO Cybersecurity
Mohammad Khaled	Ericsson
Joseph Estalilla	Federal Bureau of Investigation (FBI)
Azar Caraballo, Jeff Graves, Robert Ivanauskas	Federal Energy Regulatory Commission (FERC)
Robert Salvia	Fortress Information Security
Daniel Carbonaro, Matthew Jones, Paul Morris, William Salamon	General Services Administration (GSA)
Brian Lane, Luis Hernandez, Todd Campbell	Health and Human Services (HHS)
Trey Hodgkins	Hodgkins Consulting
Thomas Gardner	HP
Jessica Sweet	Hunter Strategy

Bill Green, Kathryn Ignaszewski	International Business Machines Corporation (IBM)
Shannon Eggers, Virginia Wright	Idaho National Labs
John Weiler	IT Acquisition Advisory Counsel
Stephanie Travers	Lumen
Edna Conway	Microsoft
Lee Szilagyi, Robert Martin, Thomas Comeau	MITRE
Omid Ghaffari-Tabrizi	Monument Advocacy
Kanitra Tyler, Thomas Doggett	National Aeronautics and Space Administration (NASA)
Sridhar Balasubramanian	NetApp
Kathryn Basinsky, Megan Doscher	National Telecommunications and Information Administration (NTIA)
Coleman Mehta	Palo Alto Networks
Ashlee Adame, Cody Marcus, Jessica Smith	Pacific Northwest National Laboratory (PNNL)
Alexa Lee	Qualcomm
Carol Woody	Software Engineering Institute
Sydney White	T-Mobile
Ahmed Shahid, Francis Addai, Heather Scott, Shane Hubble, Zetra Batiste	U.S. Department of State
Ismael Garcia	U.S. Nuclear Regulatory Commission
Anita Pantankar-Stoll, Chris Oatway, Jennifer Canlas, Steve Baum	Verizon

PRODUCT SURVEY

The Cybersecurity and Infrastructure Security Agency's National Risk Management Center welcomes your feedback. Please complete the following product survey at https://forms.office.com/g/addFVE2WHm, or scan the QR code below:

DHS POINT OF CONTACT

National Risk Management Center
Cybersecurity and Infrastructure Security Agency
U.S. Department of Homeland Security
NRMC@hq.dhs.gov
For more information about NRMC, visit https://www.cisa.gov/about/divisions-offices/national-risk-management-center.

[1] Cybersecurity and Infrastructure Security Agency, Communications Sector Coordinating Council, Information Technology Sector Coordinating Council - Information and Communications Technology Supply Chain Risk Management Task Force, Threat Evaluation Working Group, “Supplier, Products, and Services Threat Evaluation: Version 3.0,” July 2021. https://www.cisa.gov/sites/default/files/publications/ict-scrm-task-force-threat-scenarios-report-v3.pdf. Accessed on May 30, 2023.

[2] Cybersecurity and Infrastructure Security Agency, Communications Sector Coordinating Council, Information Technology Sector Coordinating Council - Information and Communications Technology Supply Chain Risk Management Task Force, Study Group,“Building a More Resilient ICT Supply Chain: Lessons Learned During the COVID-19 Pandemic,” November 2020. https://www.cisa.gov/sites/default/files/publications/lessons-learned-during-covid-19-pandemic_508.pdf. Accessed on May 30, 2023.

[3] U.S. Customs and Border Protection, “Uyghur Forced Labor Prevention Act,” Last modified on March 24, 2023. https://www.cbp.gov/trade/forced-labor/UFLPA. Accessed on June 1, 2023.

[4] National Telecommunications and Information Administration, “Software Identification Challenges and Guidance,” https://ntia.gov/sites/default/files/publications/ntia_sbom_software_identity-2021mar30_0.pdf. Accessed on June 1, 2023.