A Hardware Bill of Materials Framework for Supply Chain Risk Management

OVERVIEW

The Cybersecurity and Infrastructure Security Agency's (CISA) Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force[1] has identified and provided recommendations to address the economic and security risks associated with equipment components that may be untrusted, compromised, or subject to availability risks by creating the document entitled, *A Hardware Bill of Materials (HBOM) Framework for Supply Chain Risk Management.* The product is aimed at creating a consistent, repeatable way for vendors to communicate to purchasers the hardware components in products that they have or may purchase, enabling purchasers to evaluate and mitigate risks in their supply chain.

BENEFITS OF HBOMs

When purchasing hardware, it is crucial for a company to consider the utilization of an HBOM in order to make informed decisions regarding safe and secure hardware. *A Hardware Bill of Materials (HBOM) Framework for Supply Chain Risk Management* provides several benefits to the consumer by creating a consistent, repeatable way for vendors to communicate with purchasers about the hardware components in products that they have or will acquire in the future. This supports purchasers in the evaluation and mitigation of risks in their supply chain. Several additional benefits the framework addresses include:

- Provides a useful tool to help industry and government evaluate and address supply chain risks
- Helps organizations illuminate supply chains and support the efficient evaluation and mitigation of certain risks
- Provides portability between suppliers and purchasers

RECOMMENDATIONS FOR AN HBOM USE CASE

Requesting HBOMs is one of the many activities that purchasers can leverage to evaluate their supply chains in order to mitigate risk. Currently available HBOM formats need supplemental assistance to be portable between suppliers and purchasers and as such, this HBOM framework aims to advance such interoperability. The principal HBOM "use cases" detailed in the report 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 requirements. These scenarios will help an entity with organizing the information it may need to assess the adherence to internal, industry, customer, and government 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).

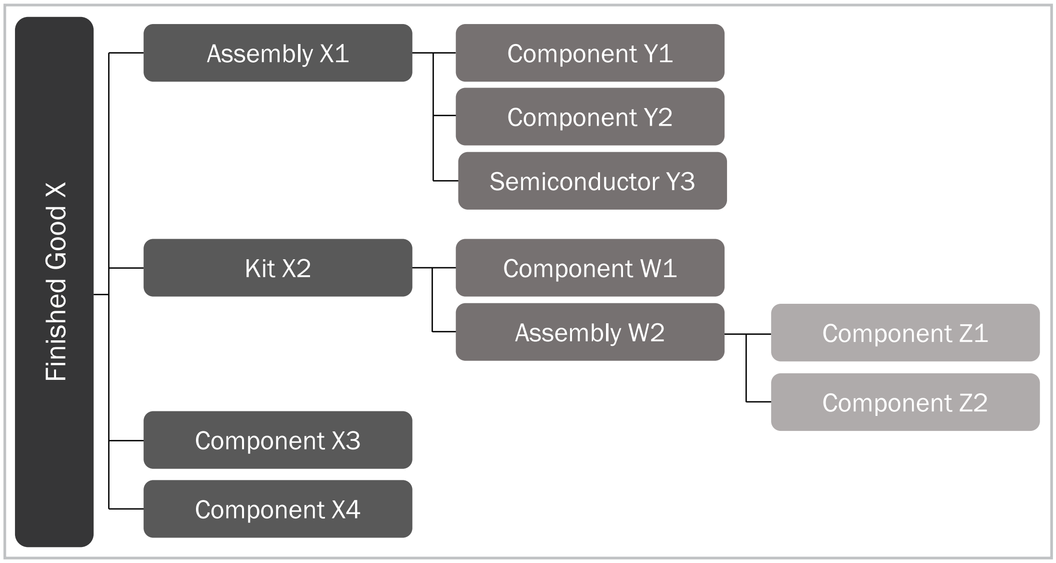
[1] The Task Force operates under, and complies with the requirements of, the Critical Infrastructure Partnership Advisory Council (CIPAC) when engaged in activities generally covered by the Federal Advisory Committee Act.

DATA FIELDS AND EXAMPLE FORMATS

This product is intended to be used on a voluntary and flexible basis and includes three key components: HBOM Use Case Categories, HBOM Formats, and a Data Field Taxonomy. Overall, this product provides definitional and formatting consistency that is helpful regardless of the specific HBOM information to be shared. It also 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).

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. This is shown in figure 1:

Figure 1: Format Example



RESOURCES

- ICT Supply Chain Risk Management Task Force: CISA.gov/ict-scrm task-force
- ICT Supply Chain Library: CISA.gov/ict-supply-chain-library
- ICT SCRM Task Force Resources: CISA.gov/ict-scrm-task-force-resources