Software Bill of Materials

Exploring a Proof-of-Concept
For the Energy Community

April 26, 2021

This meeting will be recorded.

Agenda

- Why are we here?
- SBOM Use Cases for the Energy community
- Potential Roles in a Proof of Concept
- Goals: What does "good" look like?
- Logistics for moving forward

Why are we here?

- SBOM is important
- We need to understand it as the energy community
- What this **<u>isn't</u>**
- This is your process

Why are we here?

- SBOM is important
  - And it's coming.
  - For everyone.
  - Including You.
- We need to understand it as the energy community
- What this **<u>isn't</u>**
- This is your process

Why are we here?

- SBOM is important
- We need to understand it as the energy community
    - Learning the state of play
    - Learning by doing
- What this **isn’t**
- This is your process

Why are we here?

- SBOM is important
- We need to understand it as the energy community
- What this **isn't**
    - Not a regulatory process
    - Not a biz-dev opportunity
- This is your process!

Why are we here?

- SBOM is important
- We need to understand it as the energy community
- What this **isn't**
- This is <u>**your**</u> process!
  - Please ask questions and share ideas
  - Start the conversation in the chat. It will not be shared in recording

Use Cases for SBOMs

- There are both supplier and “consumer” use cases for SBOMs.
- The suppliers probably already have a good idea of why SBOMs are helpful, but the consumers? Not so much.
- I divide consumer use cases into procuring software and operating software after it is procured and installed.
- Note that these use cases apply both to integrated devices that contain software and “standalone” software that you load on Intel-standard hardware.
- I will focus on the vulnerability management use cases, although we could discuss other use cases like licensing in future workshops.

Procurement use cases

If you can get an SBOM from a supplier whose product you're considering for purchase, you can *potentially*:

1. Identify unpatched component vulnerabilities and negotiate with the supplier about patching them.
2. Identify out-of-date or end-of-life components, and negotiate a timetable for updating or replacing them.
3. Judge the supplier:
   a) Did they provide an SBOM?
   b) Are there many unpatched component vulnerabilities?
   c) Are many components getting long in the tooth?
   d) Is there a lot the supplier doesn't know about the components?

Operating use cases

If you receive SBOMs for software you operate, you can *potentially*:

1. Identify new vulnerabilities in components and ask when the supplier will patch – or otherwise mitigate – them.*
2. When new vulnerabilities are identified (e.g. Ripple 20), determine whether they're found in any software you operate.
3. Independently mitigate a vulnerability if a patch is delayed.
4. Learn about end-of-life or out-of-date components.
5. Make risk-informed decisions to prioritize your response to vulnerabilities.

* Because a large percentage of vulnerabilities in components aren't exploitable in the product itself, it's important to learn when this is the case. This is the purpose of VEX documents.

For more information:

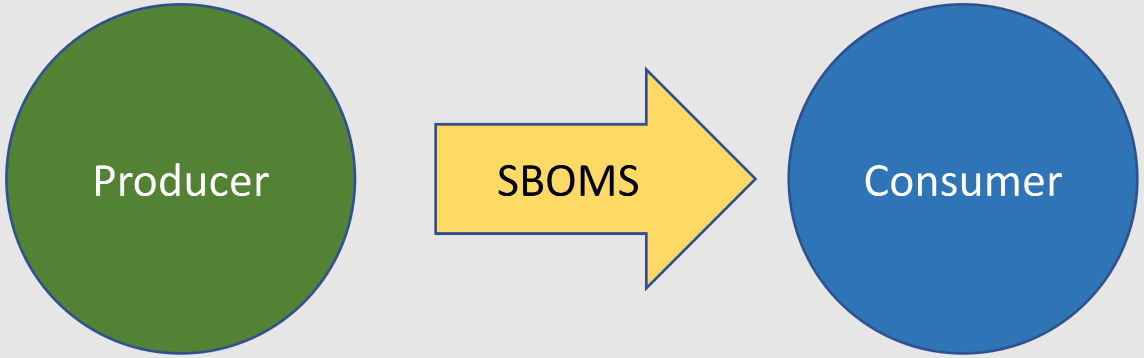
Read “Roles and Benefits for SBOM across the supply chain”

- available at https://www.ntia.gov/sbom

(or at your local SBOM retailer)

SBOM Proof of Concept Basic Model

Data exchanged by a subset of stakeholders with mutual consent

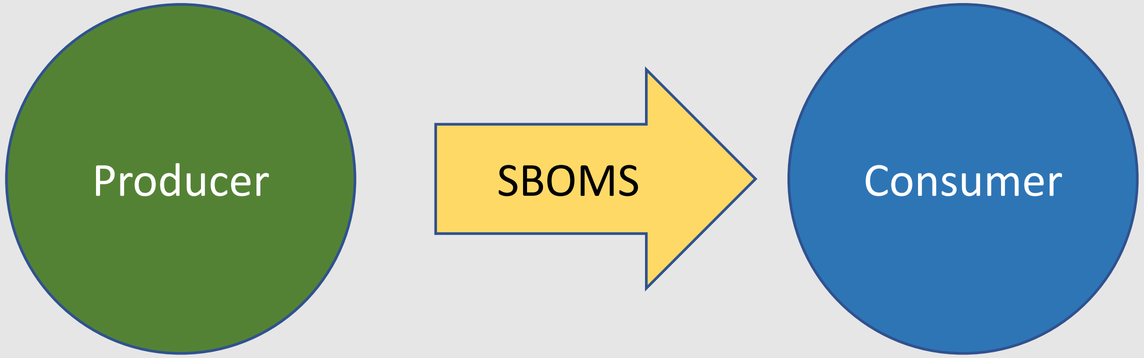


SBOM Proof of Concept Basic Model

Explore how to generate SBOMs

Define use cases for SBOM consumption

Data exchanged by a subset of stakeholders with mutual consent



Producer

SBOMS

Consumer

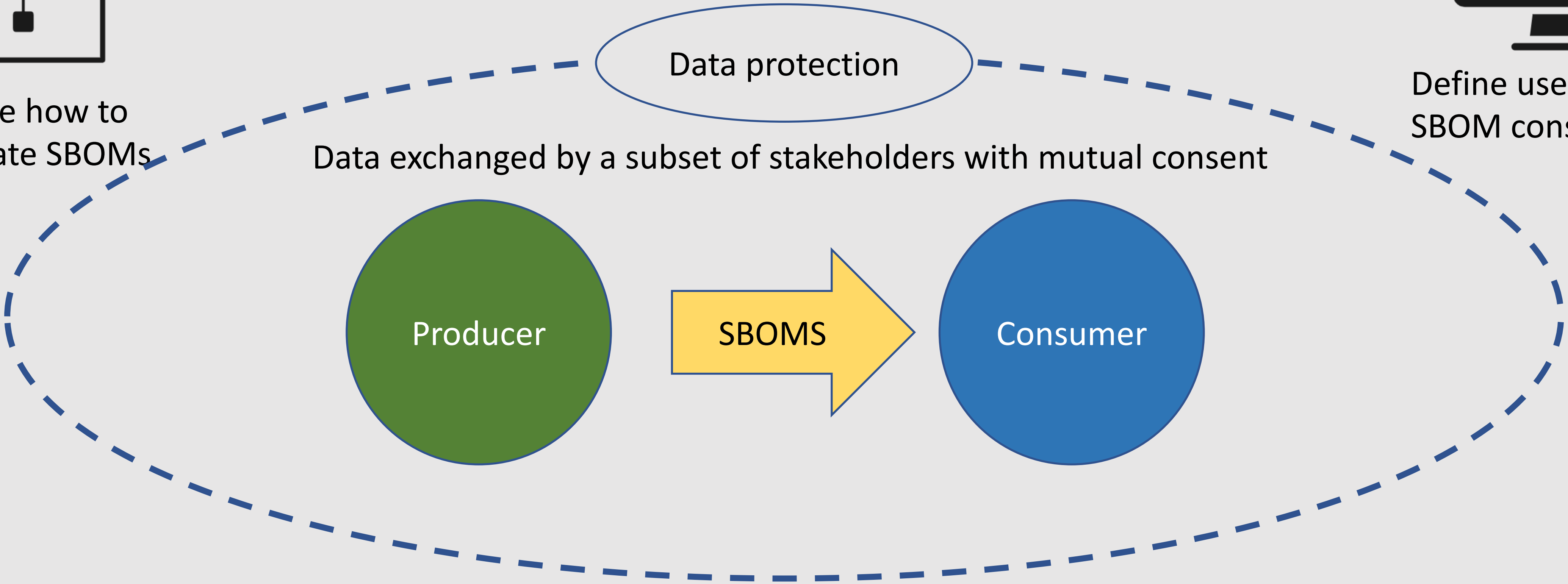
Stakeholder Community

Exercise designed by the broader energy community open to all.

SBOM Proof of Concept Basic Model

Explore how to generate SBOMs

Define use cases for SBOM consumption

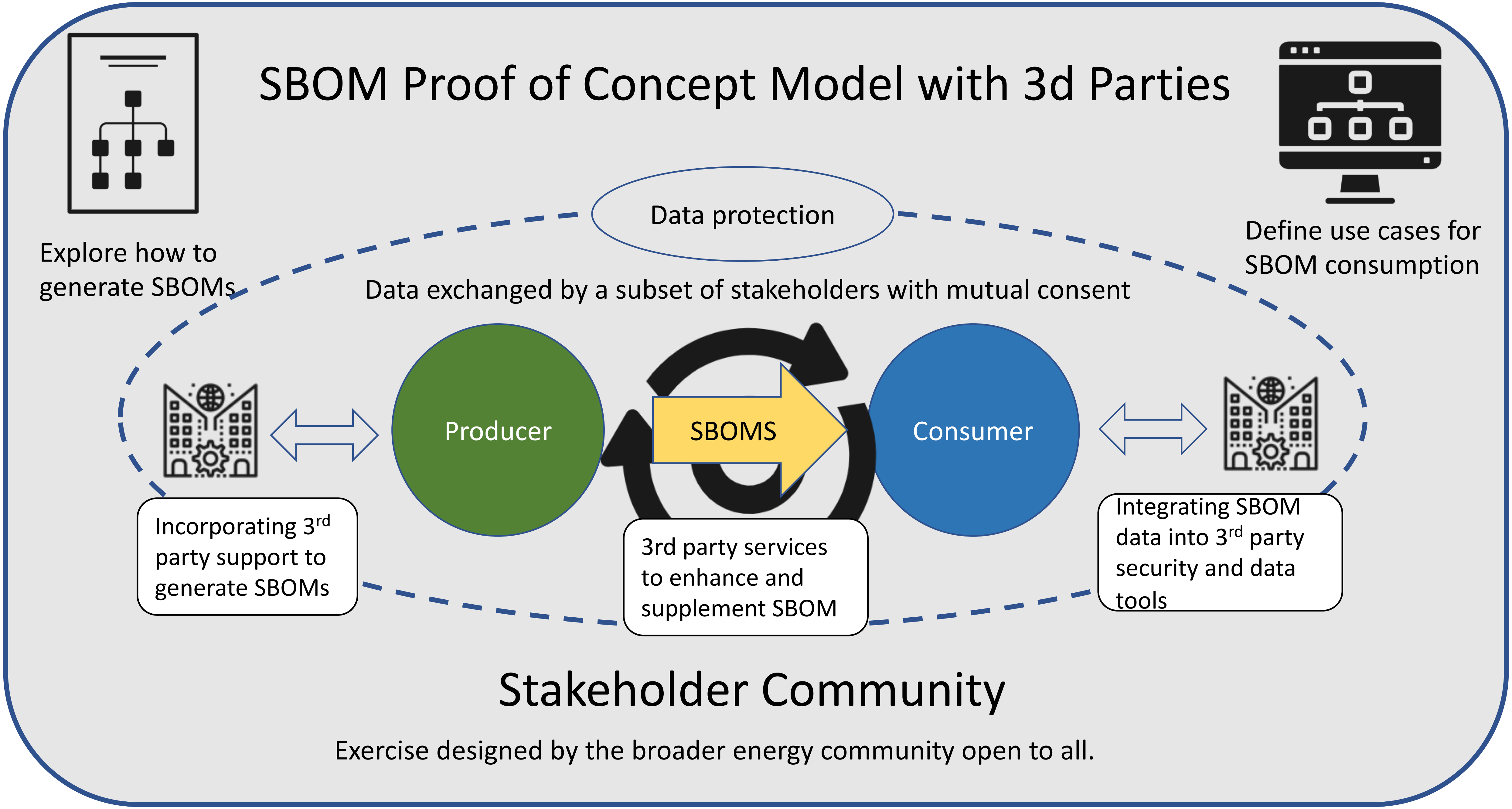


Data exchanged by a subset of stakeholders with mutual consent

Stakeholder Community

Exercise designed by the broader energy community open to all.

SBOM Proof of Concept Model with 3d Parties



Explore how to generate SBOMs

Define use cases for SBOM consumption

Data protection

Data exchanged by a subset of stakeholders with mutual consent

Producer

SBOMS

Consumer

Incorporating 3rd party support to generate SBOMs

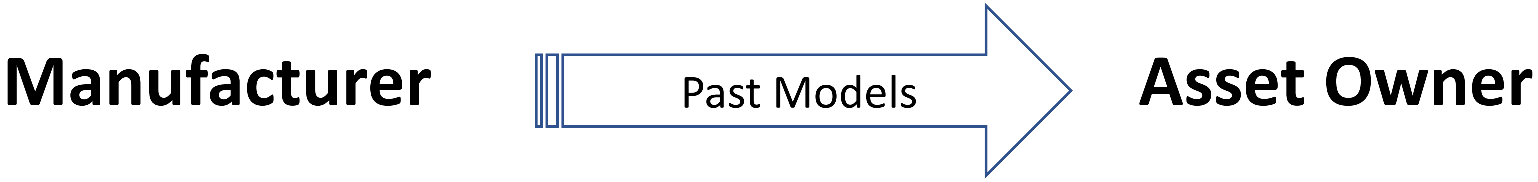
3rd party services to enhance and supplement SBOM

Integrating SBOM data into 3rd party security and data tools

Stakeholder Community

Exercise designed by the broader energy community open to all.

SBOM exchange across the ecosystem

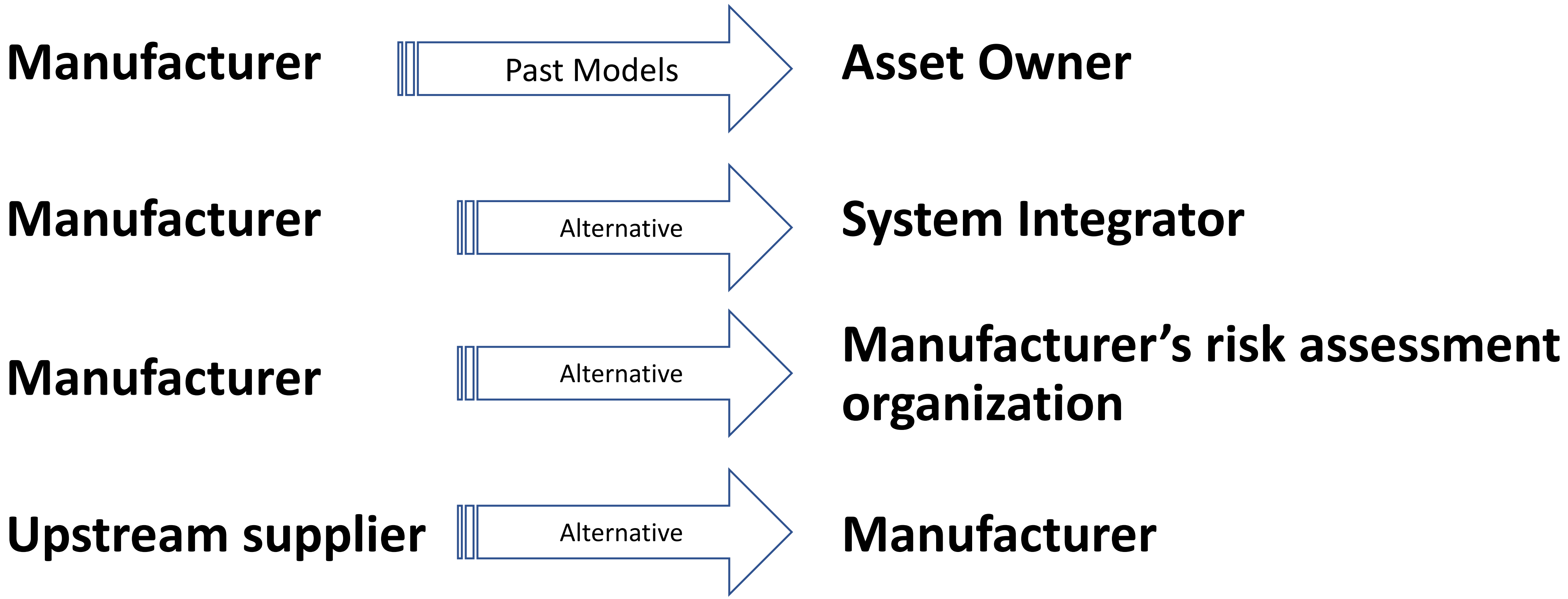


Manufacturer

Past Models

Asset Owner

SBOM exchange across the ecosystem



Manufacturer → Past Models → **Asset Owner**

Manufacturer → Alternative → **System Integrator**

Manufacturer → Alternative → **Manufacturer's risk assessment organization**

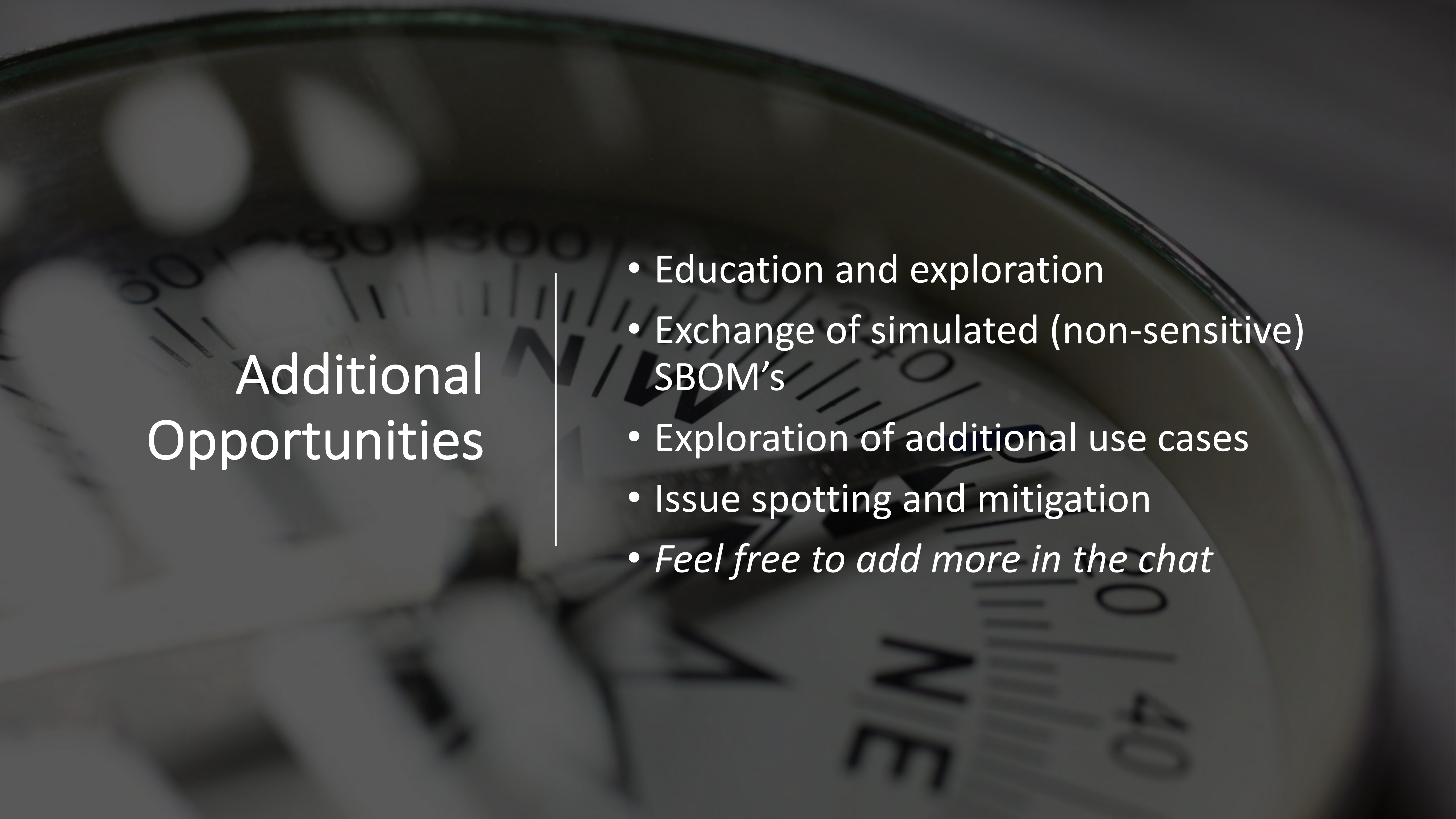
Upstream supplier → Alternative → **Manufacturer**

What Could Good Look Like?

- Past POC’s
  - Generation and publication of SBOMs for actual devices in use
  - Consumption of the SBOMs across specific use cases for acquisition and management
  - Evaluation of SBOM formats
  - Collaborative efforts to use SBOM to secure the device ecosystem.

*Pulled from NTIA SBOM Healthcare POC Report(2019)

- What else would you like to see?
  - Please respond with ideas in the chat



Additional Opportunities

- Education and exploration
- Exchange of simulated (non-sensitive) SBOM’s
- Exploration of additional use cases
- Issue spotting and mitigation
- *Feel free to add more in the chat*

SBOM Producers and Consumers

- Send Email to **SBOMEnergyPOC@inl.gov** (Allan, Tom, and Ginger) for further discussion.

Logistics

- **Frequency of meetings**
  - **Every other week?**
- **Protection of conversations**
  - **Chatham House?**
  - **Traffic Light Protocol?**
- **Mailing list for POC**
- **Meeting Summaries**