Labels, SBOMs, Vulnerability Reports, Transparency Reports Oh My…

Katerina Megas – Program Manager, Cybersecurity for the Internet of Things
Angela Smith -- Technical Lead – Cybersecurity Supply Chain Risk Management Program

NIST

19 April 2023

National Institute of Standards and Technology
U.S. Department of Commerce

Transparency is the watchword of the hour

“Embrace radical transparency and accountability”

“Organizations should expect transparency from their technology suppliers about their internal control posture as well as their roadmap towards adopting Secure-by-Design and Secure-by-Default practices.”

“Organizations should prioritize cloud providers that are transparent about their security posture”

Shifting the Balance of Cybersecurity Risk:
Principles and Approaches for Security-by-Design and -Default

-- DHS CISA + 5-Eyes Agencies, 13 April 2023

A consistent framing to think about transparency can support better cybersecurity

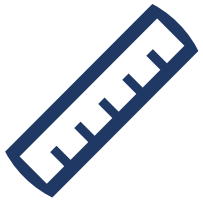
- Structured approach to providing information and actions to support secure product usage
- Enable informed choices by acquirers of connected products
- Develop a shared lexicon around transparency
- Encourage transparency to reduce information gaps, which can promote trust and help mitigate risks
- Envisioned as a tool for sharing information/expectations across the supply chain. E.g.
  - Guiding communications tailored for different kinds of audiences
  - Supporting product developers communicating with customers, regulators, conformance assessment bodies, other third parties who need to understand the product

1 - Determine the **target audience** of the information.

2 - Define the **purpose** for delivering the information to the audience.

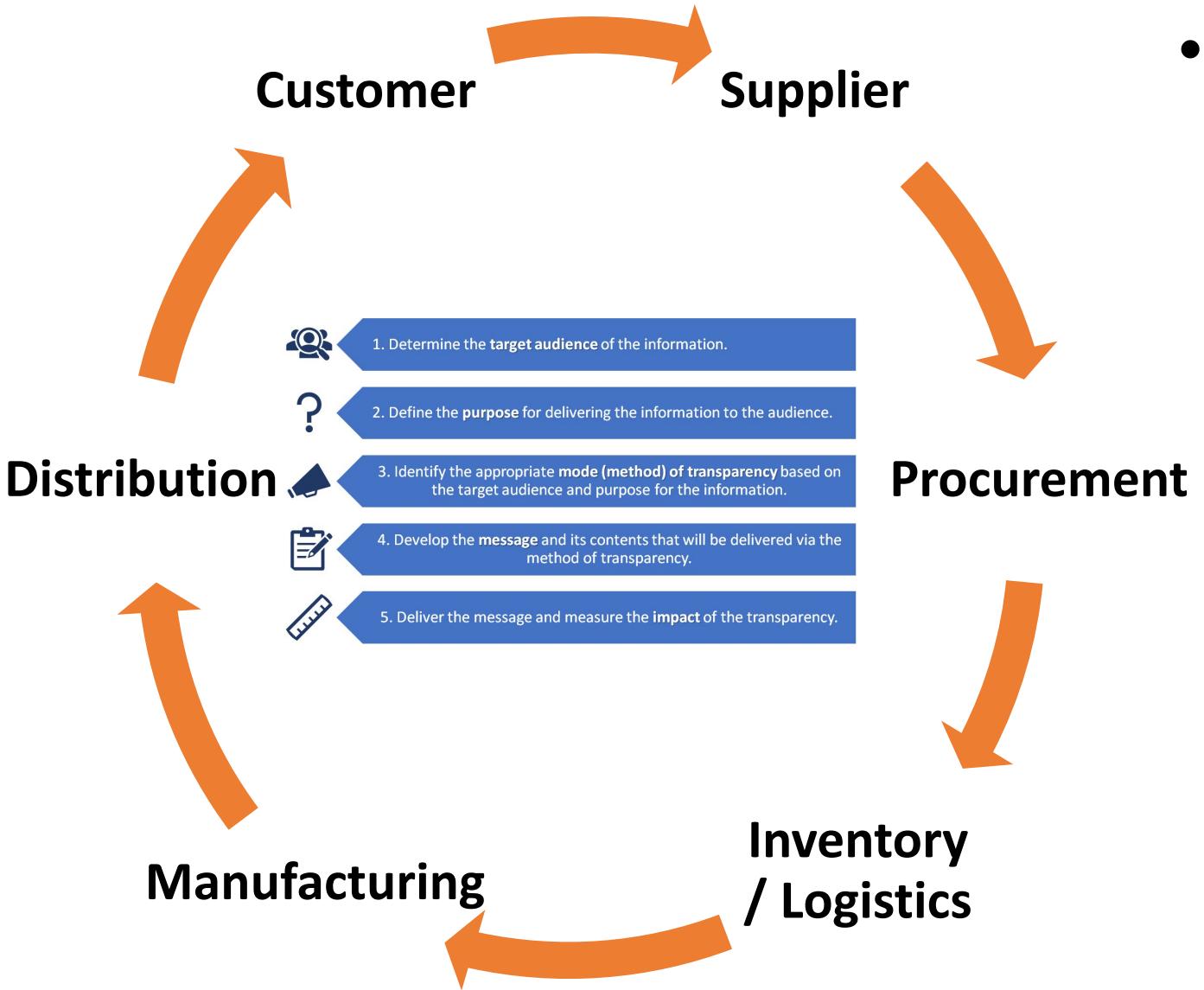
3 - Identify the appropriate **mode (method) of transparency** based on the target audience and purpose for the information.

4 - Develop the **message** and its contents that will be delivered via the method of transparency.



5 - Deliver the message and assess the **impact** of the transparency.

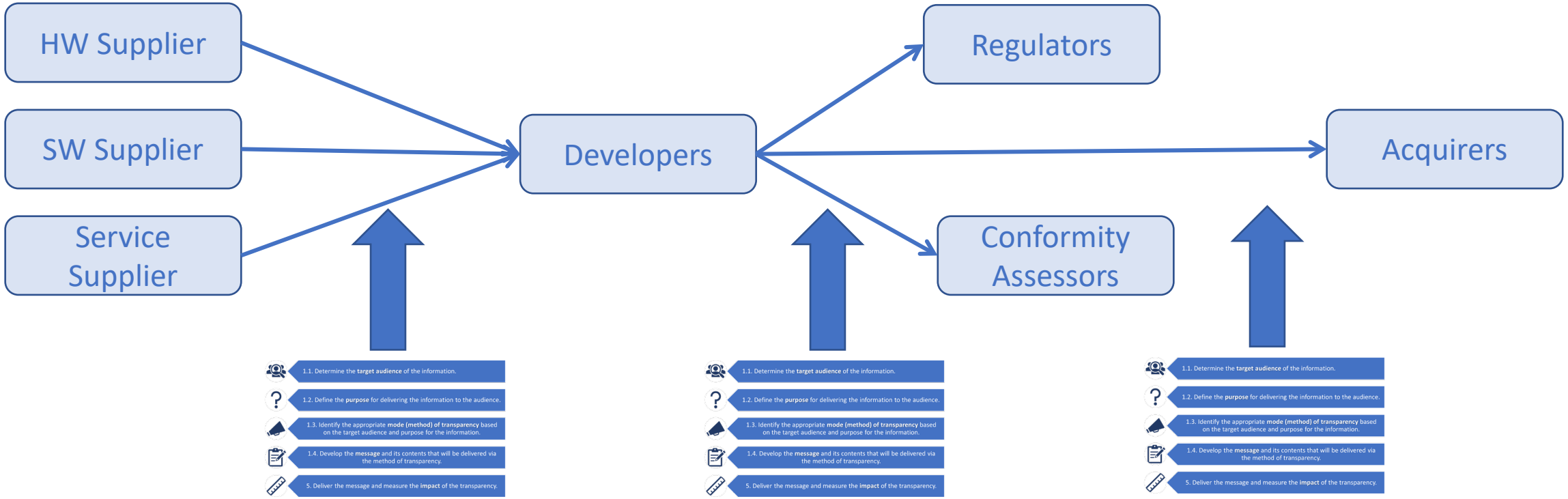
A tool for the connected product ecosystem



- Enable communication between stakeholders from different perspectives across the product ecosystem such as:
  - Producers
  - Suppliers and Vendors
  - Regulators and Conformance Assessment Bodies
  - Customers of different organizational size
    - From home customers to governments

Example of communication needs along connected product ecosystem

A Consistent Approach Applied to Information Exchanges Throughout The Supply Chain



- Enable communication between stakeholders from different perspectives across the product ecosystem such as:
  - Producers
  - Suppliers and Vendors
  - Regulators and
  - Conformance Assessment Bodies

Considerations

- What kinds of additional guidance can help stakeholders provide transparency in effective and consistent ways?
- Which existing standards, resources, and/or best-practices can help and/or inform this effort?
  - Areas of interest:
    - Taxonomy of target audiences
    - Modes/methods of transparency (e.g., SBOM, labels, technical vs. non-technical methods)
    - How to assess impact

Next Steps

- Build out these ideas and highlight key points for community input and buy-in

Release Discussion Essay

Socialize the Approach

- Meetings, workshops and other engagements with the community

Draft *Connected Product Transparency Framework*

- Additional meetings and workshops
- Additional drafts developed and released as needed by the community.

Further socialization working towards finalization