NTIA Software Component Transparency

Standards and Formats WG

Agenda

- Review of Charter, Goals and Objectives
- What has changed in the draft White Paper
- Work to be completed in the White Paper
- Potential next steps for the WG
- Open questions and needed feedback

Charter of the Standards and Formats WG

Investigate existing standards and initiatives as they apply to identifying the external components and shared libraries, commercial or open source,
used in the construction of software products.
The group will analyze efforts underway in the community and industry related to assuring this transparency is readily available in a machine-readable manner.

What Does Success Look Like?

- Machine Readable Format that:
  - Provides direct linkage to software publisher and components
  - Signed by the publisher
  - Automatable by potential products including vulnerability management tools
    - Provides data that can be used to automate enforcement of policies and processes
  - Verifiable to the package it represents
- Documented capabilities and ways to interpret it
- Useful in both the Open Source and to Commercial Product Vendor communities
- Actionable in that software publishers can implement in a lightweight fashion
- Should be a integrated part of a software publisher's development process to there is extremely low maintenance involved in keeping it current

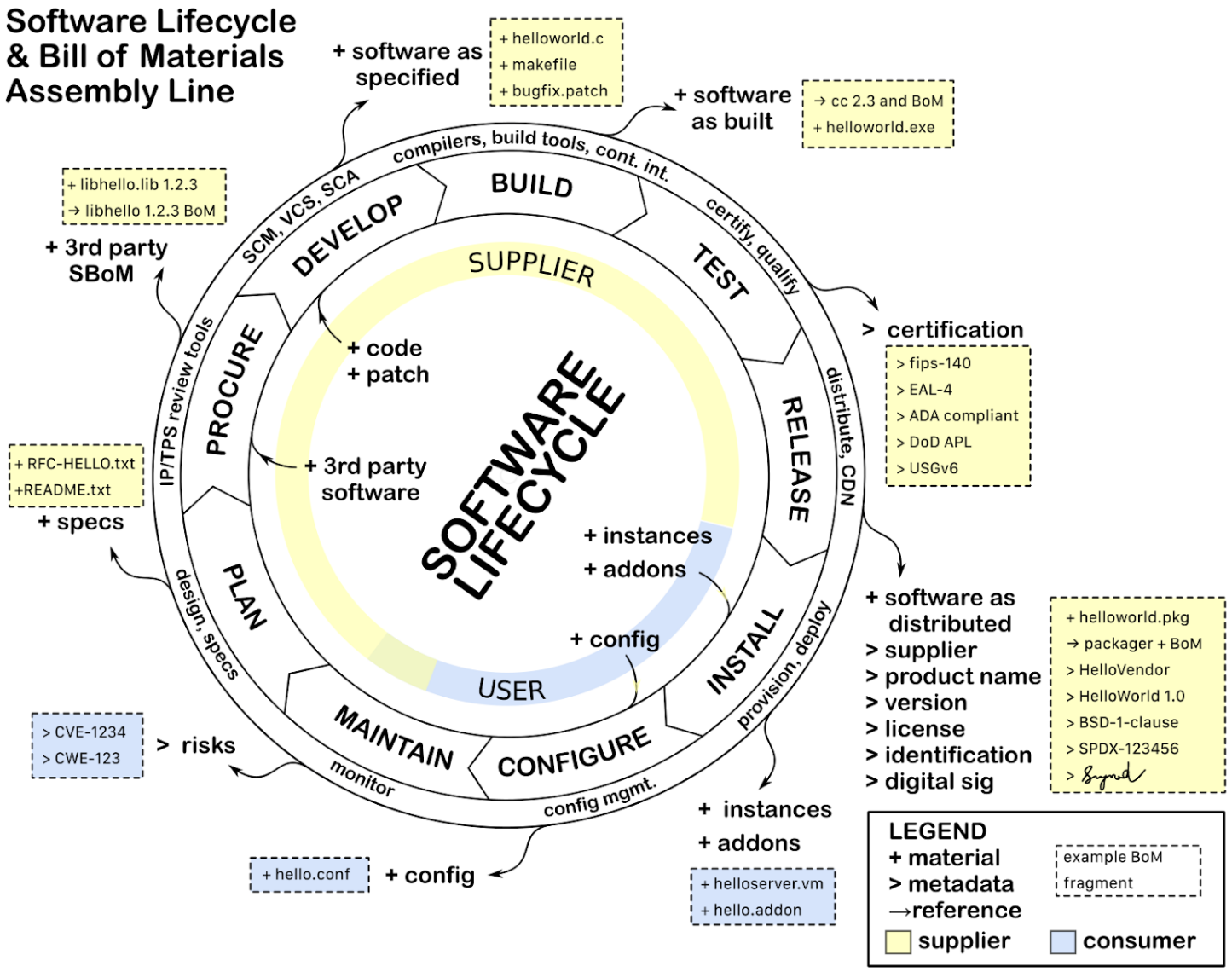
What’s new in the White Paper draft

- Explicit goals
- Lifecycle of the SBoM
- Translation and Harmonization
- Example scenario

Initial goals

- Investigate the options available today
- Document workable and actionable machine-readable formats
- Acknowledge that no single solution/format will be required (i.e. “proclaim a winner”)
- Determine how the solutions can work in harmony, since different formats were designed to address the requirements of different constituencies (e.g. developers, CFOs managing software entitlements), and mapping between well-documented formats is technically feasible.
- Support International feedback and buy-in to solutions as this is not just a US problem, and participation in this process is global.

- ***There is a Win-Win for all – our job is to find it***



SBoMs

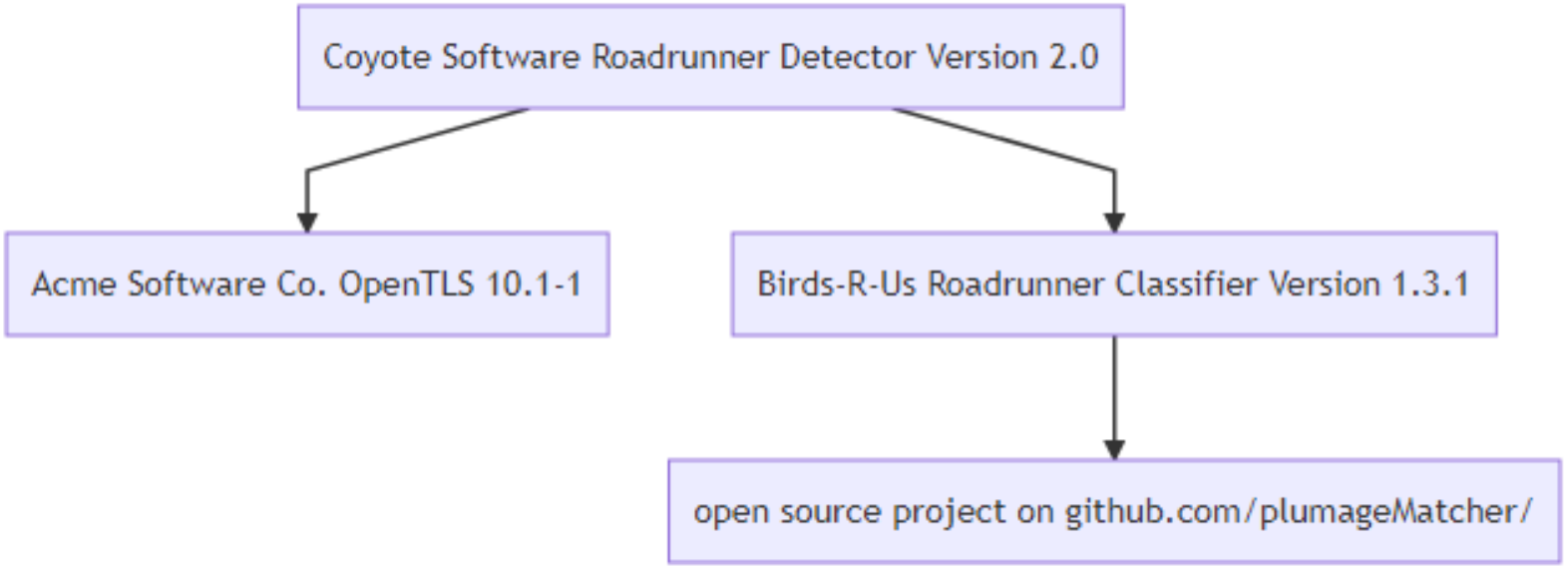
- How to produce
- How to deliver
- How to update
- How to consume

The Software lifecycle with multiple stages where underlying code might change, and thus the SBoM would be updated to reflect the changes.

Mapping the Baseline Component Information

Field	Represented in SPDX	Represented in SWID
Supplier	(3.5) PackageSupplier:	<Entity> @role (softwareCreator/publisher), @name
Component	(3.1) PackageName:	<softwareIdentity> @name
Unique Identifier	(3.2) SPDXID	<softwareIdentity> @tagID
Version	(3.3) PackageVersion:	<softwareIdentity> @version
Component Hash	(3.10) PackageChecksum:	<Payload>/../<File> @[hash-algorithm]:hash
Relationship	(7.1) Relationship:	<Link>@rel, @href
SBOM Author	(2.8) Creator	<Entity> @role (tagCreator), @name

Toy Example Scenario



Goals

- Lightweight: easy to read in a document.
- Captures the basics of dependencies.
- Can be extended to capture edge cases.

Work to be completed in the White Paper

- Finish example with SPDX and SWID formats
- Synchronize with the Framing group’s Basic Component Information
- Validate against Use Case benefits
- Incorporate outstanding comments and feedback from stakeholders

Potential next steps for the working group

- Tooling
- A “quick start guide”
  - Examples and Reference Implementations
  - Debating value of a short paper vs. tools
- Discussing how to transmit/deliver SBoMs

Capturing and Documenting Tools

- Many tools exist today for both SPDX and SWID
- We want to document what exists today
- Identify gaps: languages, frameworks, sectors, etc
- Potentially create a resource where people can submit their own tools
  - Need to consider quality, risks of malicious submissions, etc

Logistics

Contacts:

- J. C. Herz (Ion Channel) jc.herz@ionchannel.io
- Kate Stewart (Linux Foundation) kstewart@linuxfoundation.org

Mailing List: ntia-sbom-formats@linuxfoundation.org

Subscribe at: https://lists.linuxfoundation.org/mailman/listinfo/ntia-sbom-formats

Shared Drive: https://drive.google.com/drive/folders/1KAQ7AWlWMKcSFnRc_S-7XB76xFRRWLmT

SPDX and SWID
Field Categories and Distribution

Category	# SPDX fields	# SWID fields
Component Identity - MVP	3	3
Component Identity - Post-MVP	3+	2+
Component Info	15	16
Description	13	17
Discovery	0	20
Entitlement & Procurements	0	6
IP Related	22	0
Mappings	6	5
SBOM Metadata	5	4
SBOM Provenance	4	3

Mappings & Relationships

Mapping Types	SPDX	SWID
between components in document	29	13
to external documents	1	1
to external sources (NVD, etc.)	2	1

NTIA Director David Redl's Blog

"It is important to note that many technical solutions developed by industry and standards experts are available, but they haven't been widely adopted. Better coordination is needed among software vendors, purchasing organizations, and security solutions providers to increase awareness of solutions and new approaches. A key objective of this process is building consensus across stakeholders on the best tools for sharing information on component data between vendors and customers."

"For the software component transparency initiatives, NTIA welcomes participation from across the digital ecosystem, including software vendors, IoT manufacturers, medical device manufacturers, enterprise customers such as the financial services community, health care delivery organizations and higher education institutions. We also encourage input from vulnerability management solution providers, information security experts, and civil society."

It is also NTIA's first step in implementing the actions put forward by government and industry stakeholders in the **Report to the President on Enhancing Resilience Against Botnets**.

https://www.ntia.doc.gov/blog/2018/ntia-launches-initiative-improve-software-component-transparency

Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats

Action 1.3 Software development tools and processes to significantly reduce the incidence of security vulnerabilities in commercial-off-the-shelf software must be more widely adopted by industry. The federal government should collaborate with industry to encourage further enhancement and application of these practices and to improve market

- "As an example, modern products use many software components, libraries, and modules, some of which may be outdated or vulnerable and are not always closely tracked by manufacturers in the rapid development cycle. While the notion of transparency around components of software is not new, wide support and adoption has not been realized. NTIA should engage diverse stakeholders in examining the strategies and policies necessary to foster a marketplace for greater software component transparency, including identifying and exploring market and other barriers that may inhibit progress in this space. Knowing what software has been incorporated into a product is a fundamental step toward being able to keep it updated and to mitigate threats when they arise.

https://www.commerce.gov/page/report-president-enhancing-resilience-against-botnets