SBOM FORMATS & STANDARDS GROUP - REPORT OUT

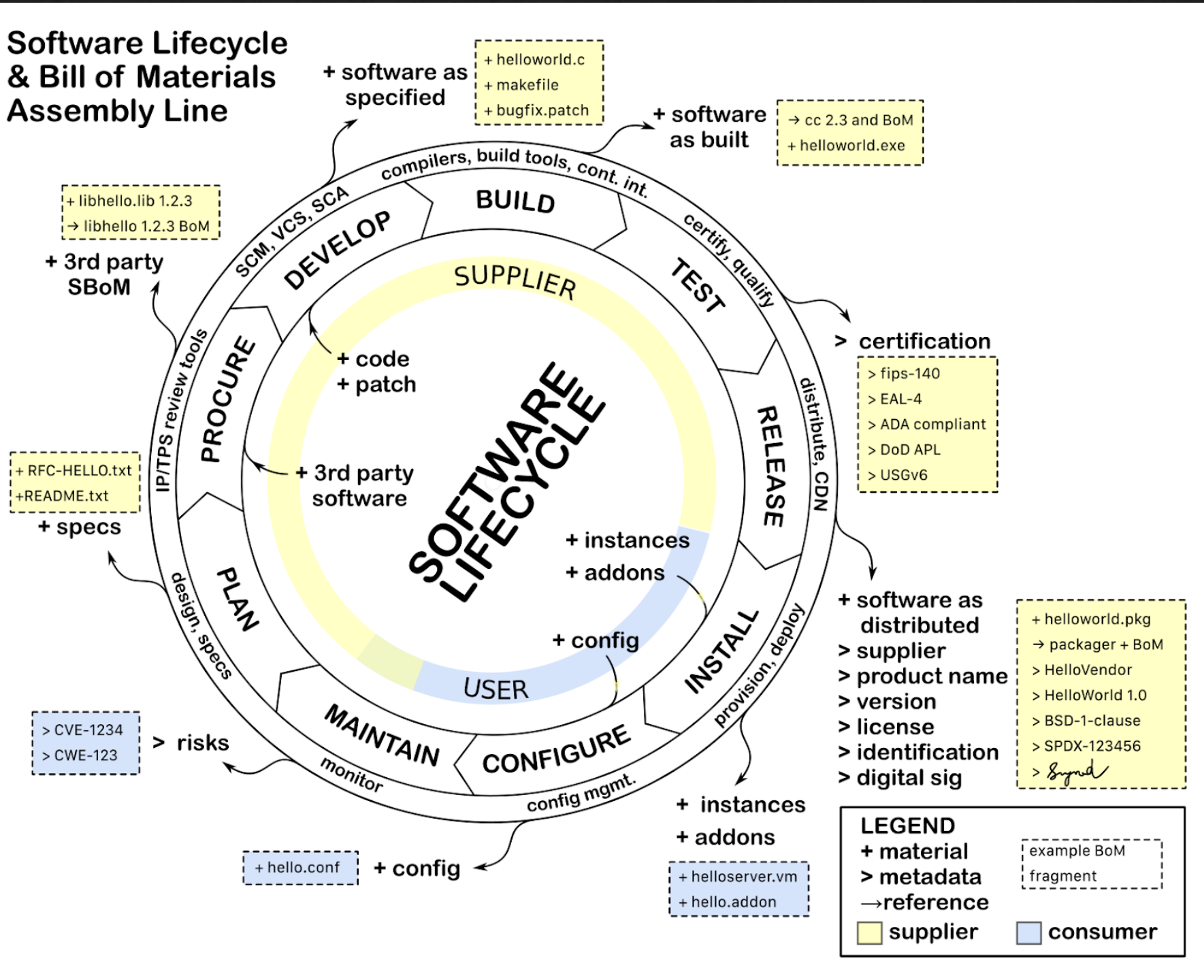
CO-CHAIRS:

JC HERZ & KATE STEWART

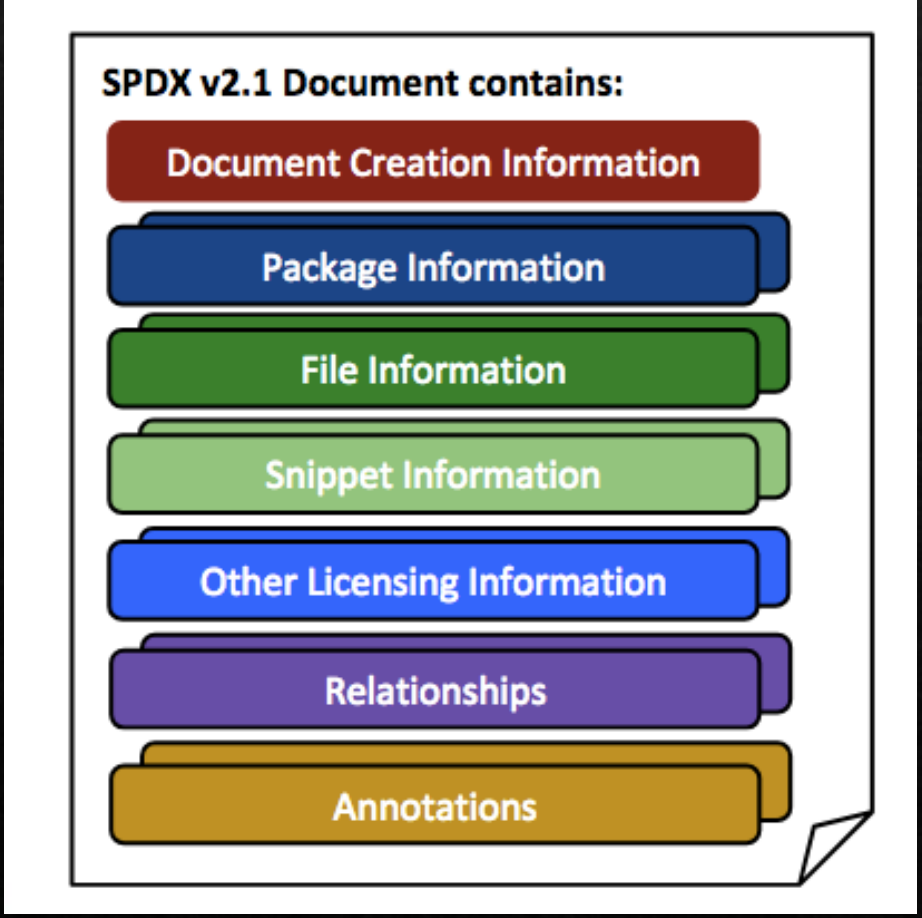
Lifecycle of an SBOM

Information that goes into SBOMs can be best obtained from the tools and processes used in each stage of the software lifecycle

1. Produce
2. Deliver
3. Update
4. Consume



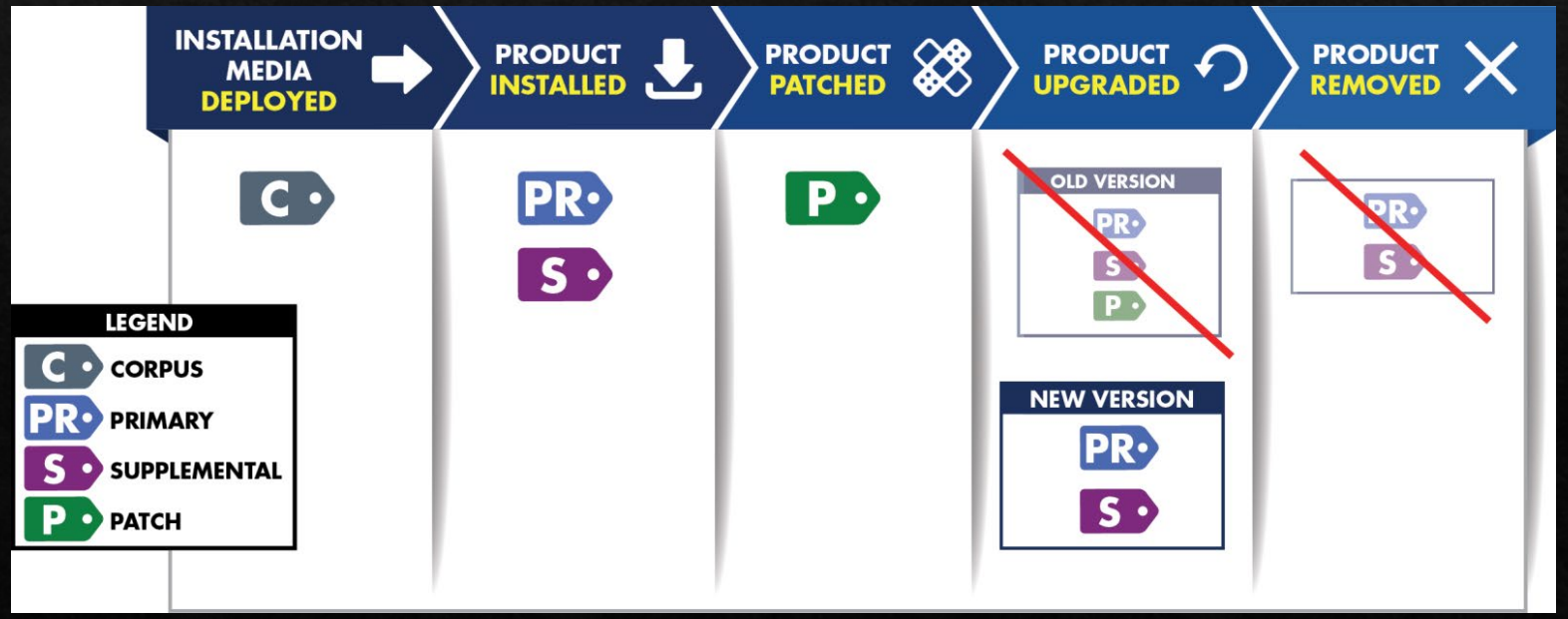
Key Format: SPDX



The Software Package Data Exchange (SPDX®) specification provides a standard language for communicating licensing and components information(metadata) for software packages and related content with the aim of facilitating license and other policy compliance between companies and organizations.

Key Format: SWID

The Software Identification (SWID) Tags were designed to provide a transparent way for organizations to track the software installed on their managed devices. It was defined by ISO in 2012 and updated as ISO/IEC 19770-2:2015 in 2015. SWID Tag files contain descriptive information about a specific release of a software product.



Translation & Harmonization Guidance for Mapping to Framing Baseline

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

Table 1: Mapping baseline component information to existing formats

Related Formats Surveyed

CoSWID Tag

CPE

Cyclone DX

Grafeas

in-toto

Package-URL (purl)

SEVA

Software Heritage Index

Sparts

SPDX-LIte

Next Steps

Tooling Support and Quick Start Guides

Working with Key Format definition groups to improve handling of:

- Software Identifier Challenges
- Delivery and Distribution
- Component Modification
- Formats for Higher Trust and Provenance