SBOM Sharing Working Group

Los Angeles, June 14, 2023

What We Are

Group of international public and private sector folks working to:

- *"Facilitating the exchange/sharing of SBOMs from legitimate sources to interested parties in ways that are fit for associated purposes."*
- Delivering actionable guidance to enable stakeholders to effectively and efficiently share SBOMs

What we are building on:

• SBOM Definition, tooling, existing implementations

Challenges:

Gopher holes

 Identity!

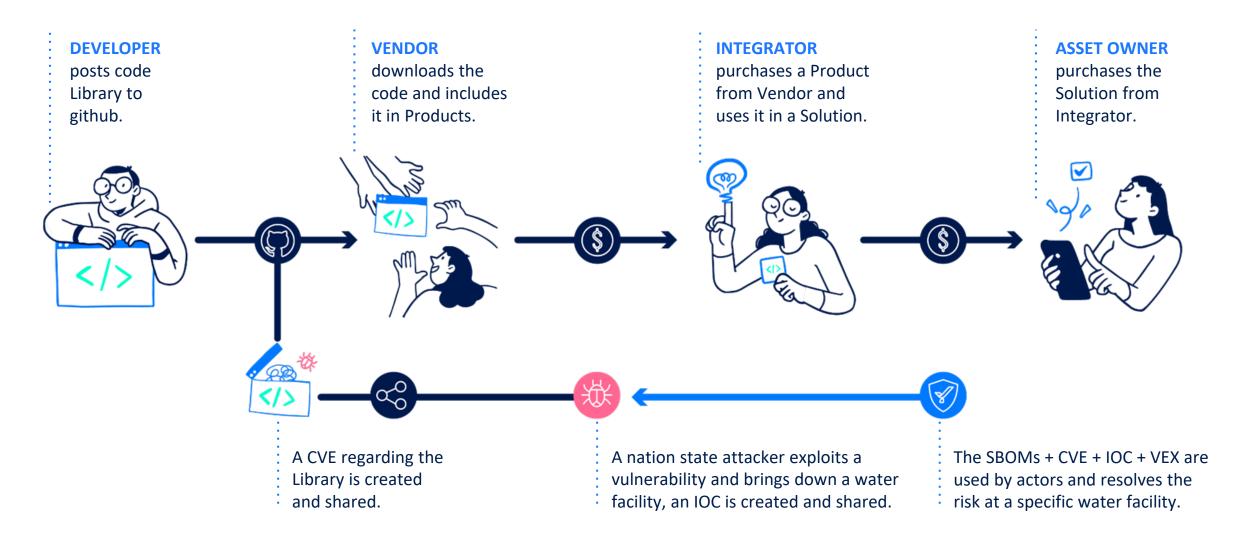
Where We Are

- Deliverables:
 - Framing Document
 - Description
 - Mechanisms
 - Stakeholders
 - One-to-one SBOM Sharing
 - Multi-party SBOM Sharing

o POCs

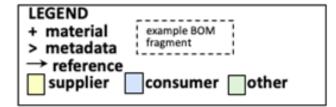
- Compilation of existing and proposed methodologies
- Demonstrations of strengths/weaknesses
- Open source, standardized, and proprietary

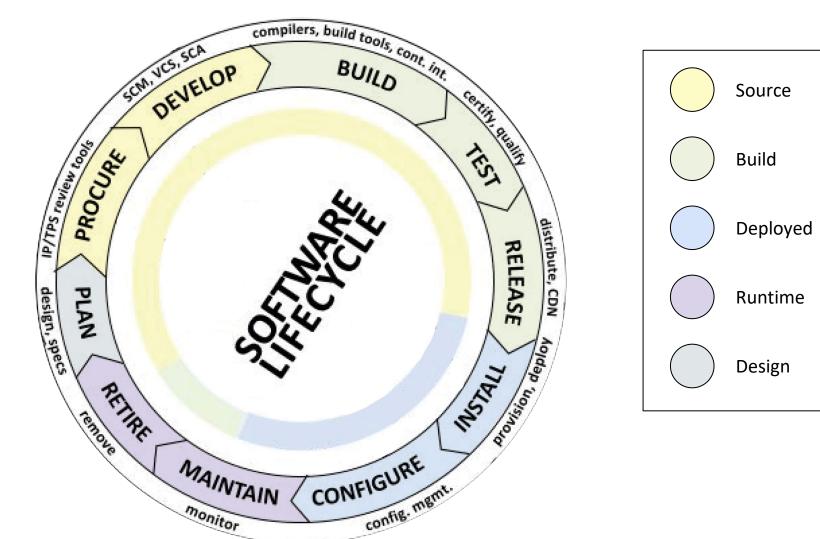
Scope of Issue



Generate SBOMs where the data is

Derived from : NTIA's Survey of Existing SBOM Formats and Standards





Electric Sector Supply Chain Stakeholders



Upstream open source



Vendor



Integrator



Regulator



Service Provider



Industry Association



Public Sector Information Sharing

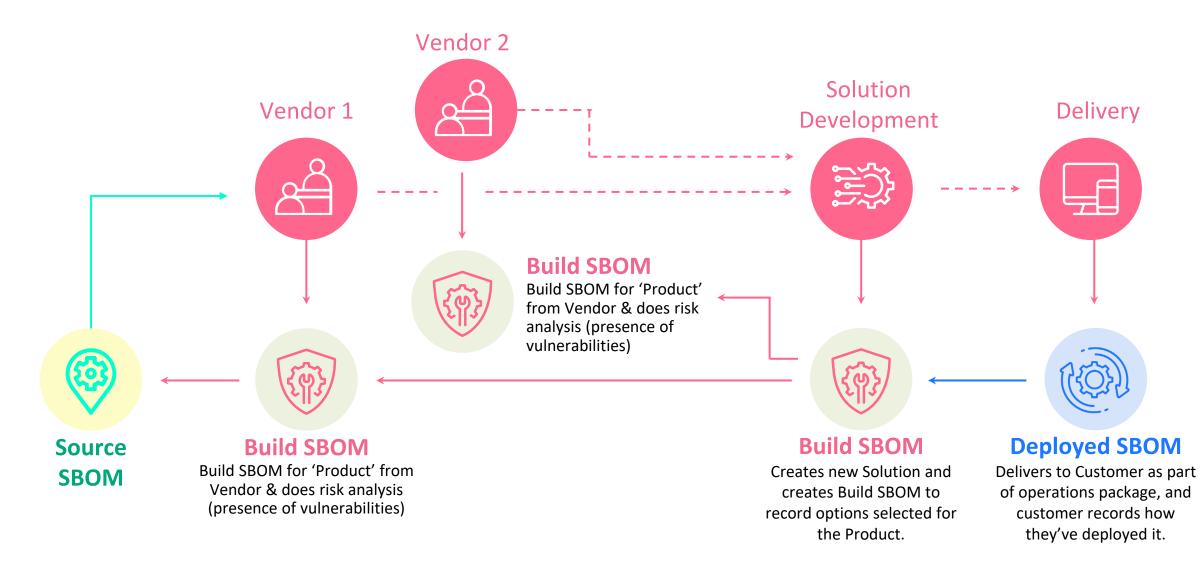


Data Value Addition Providers

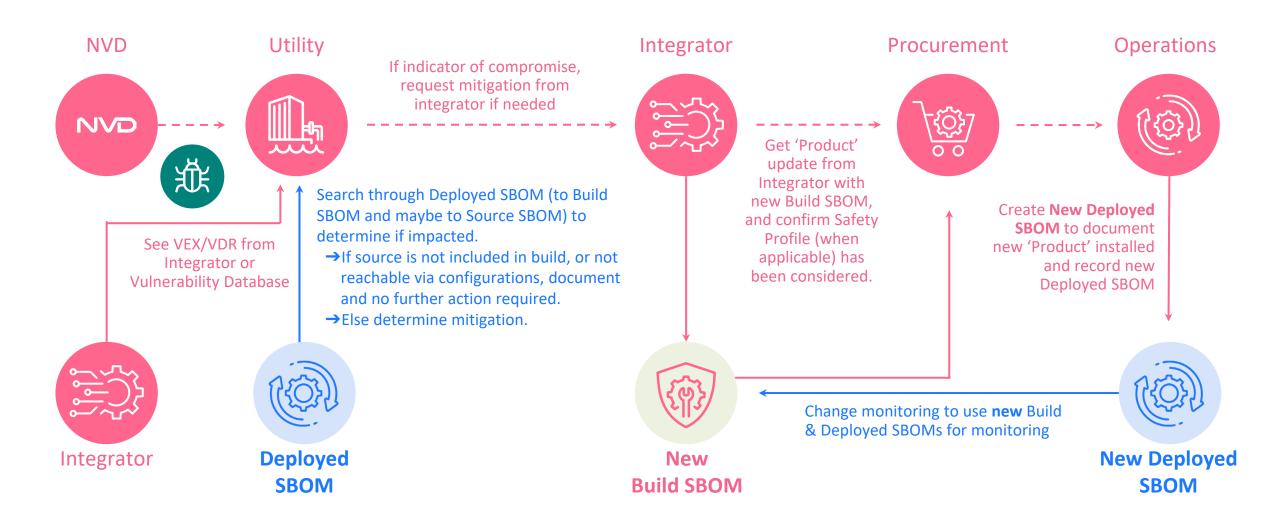




Integrator Delivering Solution



Utility managing a security fix



Supply chain intelligence shared and used

Public sector entity creates and shares IOC

OC

Vendor, Integrator, and ISAC receive IOC Established policy is performed including SBOM review, sharing, and updating

Integrator establishes monitoring

Remediation is performed by Integrator at a specific water facility.



Next Steps

- Join the group
- Participate in a POC
 - Produce, consume, share

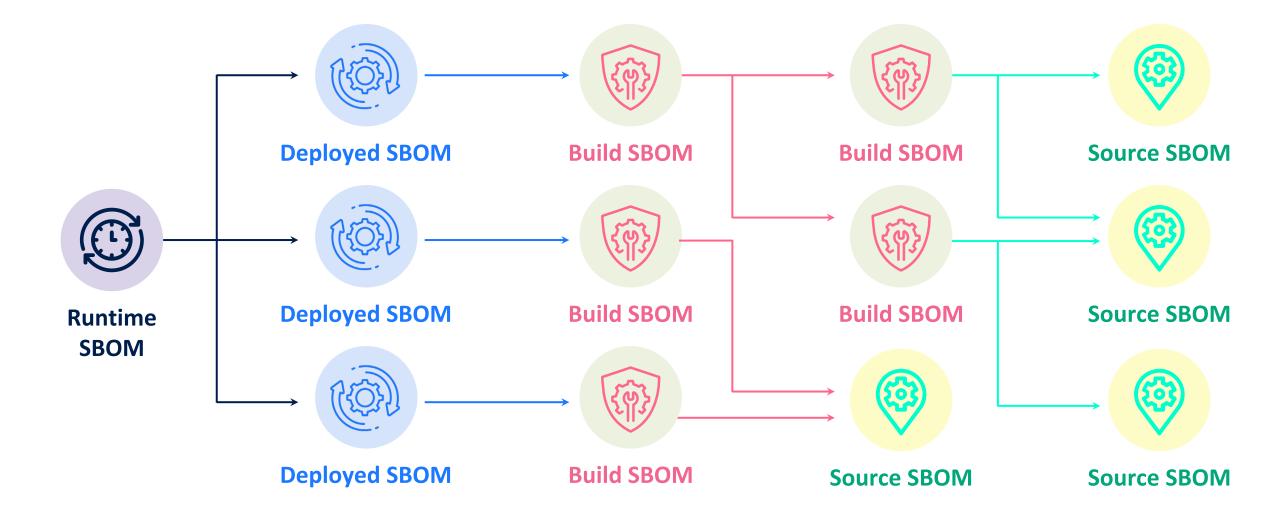
- Create content
- #cisasbomsharing

Thank You



CONTACT Chris Blask | VP Strategy chris@cybeats.com

Understanding Safety Critical System: Traceability



SBOM Creation and Consumption

+ helloworld.c + makefile + software Software Lifecycle & Bill + bugfix.patch as specified compilers, build tools, cont. in of Materials Generation + software as built + libhello.lib 1.2.3 DEVELOP → cc 2.3 and BOM BUILD → libhello 1.2.3 BOM + helloworld.exe _ _ _ _ _ _ _ _ _ _ _ _ _ entity quality + 3rd party SBOM PROCURE **LEST** code > certs IP/TPS review t + patch > fips-140 > EAL-4 -------distribute, + RFC-HELLO.txt > ADA compliant 3rd party RELEASE + README.txt > DoD APL software > USGv6 + specs → Source PLAN design GN → Binary + instances Drovision, deploy + addons 11STAL + software as REIIRE + helloworld.pkg distributed + config → Packager + BOM > replace > supplier > HelloVendor > product name USER > HelloWorld 1.0 + libehellolib 1.2.3 > version > BSD-1-clause LEGEND CONFIGURE MAINTAIN > license > SPDX-123456 + material example BOM > identification config. mgmt. > Synd fragment > metadata > risks > digital sig monitor → reference + instances > CVE 2018-5400 supplier consumer other > CWE-346 + addons + helloserver.vm + config + hello.addon

+ hello.conf