National Telecommunications and Information Administration
[Docket No. 210527–0117]
RIN 0660–XC051
Software Bill of Materials Elements and Considerations
Request for Public Comment

Darren Rivey
darrenrivey at gmail dot com

> h. Depth. As noted above, while ideal SBOMs have the complete graph of the assembled software, not every software producer will be able or ready to share the entire graph.

The origin of software in the Open Source Software (OSS) community brings into question the identity of the contributor and its absolute origin. Details like OSS contributor Citizenship, Location, Age, and other factors are not barriers as they would be for participation in other organized activities. With OSS being highly autonomous and distributed, it is up to each project maintainer to decide how and from whom it will accept contributions [Curphey, Wheeler]. The absence of absolute software contribution origin traceability highlights ethical concerns and the sentiment that no OSS is entirely trustworthy.

Unlike traditional supply chain relationships where trusted (software) suppliers face possible contractual penalties from (software) consumers, there is no such obligation for popular OSS licenses as they are provided “as is” unilaterally [License-MIT], [License-Apache].

When the software consumer has a contractual arrangement (End User License Agreement) with a commercial provider of OSS there is a more balanced relationship. Commercial re-packaging of OSS makes it highly valuable while simultaneously opening a pathway for transmission of unforeseen risk(s).

The DHS Continuous Diagnostics and Mitigation (CDM) program is dependent on the software consumer to engage the (software) supplier to supplement initial Supplier Management and Product Assurance documentation [DHS-CDM-SCRM], **if requested**. In some acquisitions, the inclusion of an SBOM (or its relevant equivalent) and related cybersecurity elements are entirely omitted [GAO-19-128]. “And contractors are only responsible for meeting the terms written in a contract.” [GAO-21-179]. **These examples are entirely silent on depth and traceability to the absolute software origin.**

> 4. Flexibility of implementation and potential requirements. If there are legitimate reasons why the above elements might be difficult to adopt or use for certain technologies, industries, or communities, how might the goals and use cases described above be fulfilled through alternate means? What

```
accommodations and alternate
approaches can deliver benefits while
allowing for flexibility?
```

Small- and medium-sized businesses carry a proportional more significant financial burden for compliance with laws and regulations. This makes them possible targets of espionage activity contrary to the nation's interests [Priestap, Triplett], [NIST-800-161r1]. While it is normal for each business entity to be responsible for itself, there is a compelling reason [DOT&E] to take an alternative collectivist approach for those that are in any way related to the best interests of the nation. Unlike one-time efforts to check a box (example: FIPS 140-2, -3), the SBOM effort must be sustained, continuous, tolerate acceptable risks, and include independent auditor oversight (example: FedRAMP Moderate and High).

References

[Curphey, Wheeler] Improving Trust and Security in Open Source Projects, The Linux Foundation, Third Edition, Know Your Users, p9, https://www.linuxfoundation.org/wp-content/uploads/improving_trust_security_in_oss_projects.pdf

[License-MIT] The MIT License (spdx MIT), https://opensource.org/licenses/MIT

[License-Apache] Apache License, Version 2.0 (spdx Apache-2.0), https://opensource.org/licenses/Apache-2.0

[DHS-CDM-SCRM] US DHS CDM Approved Products List *Attachment A Supply Chain Risk Management,* https://www.gsa.gov/technology/technology-products-services/it-security/continuous-diagnostics-mitigation-cdm/continuous-diagnostics-mitigation-cdm-tools-special-item-number-sin-information-for-vendors

[GAO-19-128] Weapon Systems Cybersecurity: DOD Just Beginning to Grapple with Scale of Vulnerabilities, https://www.gao.gov/products/gao-19-128

[GAO-21-179] Weapon Systems Cybersecurity: Guidance Would Help DOD Programs Better Communicate Requirements to Contractors, https://www.gao.gov/products/gao-21-179

[Priestap, Triplett] The Espionage Threat to U.S. Businesses, https://www.lawfareblog.com/espionage-threat-us-businesses

[NIST-800-161r1] Cyber Supply Chain Risk Management Practices for Systems and Organizations, Lines 5989-6102, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1-draft.pdf

[DOT&E] FY20 Annual Report for the Office of the Director, Operational Test & Evaluation, "*Nearly every warfighting and business capability is now software-defined*.", p III, https://www.dote.osd.mil/Portals/97/pub/reports/FY2020/other/2020DOTEAnnualReport.pdf