OpenUK's response to NTIA request for information on the use of SBOMs

17th June 2021

Attn: Evelyn L. Remaley, Acting NTIA Administrator

OpenUK welcomes the Executive Order 14028 on Improving the Nation's Cybersecurity dated May 12, 2021; and the NTIA's invitation to comment (Docket No. 210527–0117).

Trust in digital infrastructure requires transparency of the type created by the approach used in relation to Open Technologies. The open source software community is ideally placed to respond to the challenges that the NTIA is seeking to address in supply chain through the use of Software Bill of Materials ("**SBOMs**"), and stands ready with over a decade of commercial governance experience in effective enterprise-level code governance.

The open source software community operates in the context of the successful development, deployment, and adoption of technology and in governance and de facto standards keeping pace with innovation, including: (i) SPDX, the de-facto standard in relation to SBOMs that is currently submitted for publication as an ISO standard; and (ii) OpenChain (ISO 5230:2020), the process management standard for open source licence compliance. Another key element of governance common in the open source software community is the existence of established industry governance and legal organisations with high levels of collective expertise, such as OpenUK's legal and policy group on whose behalf this response is submitted. These organisations offer a wealth of experience in open source software supply chain management and operate in a collaborative model as with the associated software community.

Good practice in the modern open source software community enables the production and sharing of information such as the SBOM, facilitating traceability in respect of vulnerabilities and for the purposes of licence compliance. Whilst SBOMs should include information as to the origins of code, we do not see any value in SBOMs as requiring the disclosure of individuals engaged in the development of components.

The open source software community's high level of good housekeeping in governance has led it to have a deep understanding of its code base that may well not be matched amongst proprietary software providers. The high degree of source code auditability and peer review from its open nature, gives a rigour to vulnerability testing that is undoubtedly unmatched. We note that basing trust in infrastructure, on the provision of an SBOM, in the absence of transparent and open source code auditability, implies a requirement of trust in the accuracy of its content and the information provided by all proprietary software vendors.

Software vendors should all be held to the same standards with regard to their products as are already met by the open source software community distributed code, when it comes to transparency and trust, including the disclosure of components and their origin, and source code auditability. We believe this does not merely extend to distributed software and software-as-a-service, but also to other cloud and platform delivery models (e.g., IaaS, PaaS, etc).

In response to the challenges raised in the Executive Order, the software industry now needs to implement new ways of managing software. The open source software community comprises a number of highly successful self-managing communities (many of which are business communities), and much can be learned from them.

Chris Eastham
Chief Legal Officer, OpenUK