We welcome 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 infrastructure requires transparency, of the type provided by the approaches used in relation to Open technologies. The Open community is ideally placed to respond to the challenges that the NTIA is seeking to address when it comes to SBOMs, and stands ready with more than a decade of experience in effective enterprise-level code governance.

The Open community operates in the context of the successful development, deployment, and adoption of technology and standards keeping pace with innovation, including: (i) SPDX, the de-facto standard in relation to SBOMs that is currently being 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 community is the existence of established industry organisations with high levels of collective expertise, such as OpenUK's legal and policy group on whose behalf this response is submitted.

Good practice in the modern Open 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 SBOMs as requiring the disclosure of individuals engaged in the development of components.

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

Software vendors should be held to the same standards with regard to their products as are already met by the Open community 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 other cloud 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 community comprises a number of highly successful self-managing communities (many of which are business communities), and much can be learned from them.