From: The Open Source Initiative (OSI)
To: The National Institute of Standards and Technology (NIST)
Date: May 26, 2021
Subject: Position Statement on Guidelines for software integrity chains and provenance

---

The Open Source Initiative[1] is a California 501(c)(3) established in 1998 and steward of the Open Source Definition, the criteria used to determine whether a software license can be called "open source." OSI works to promote the public understanding and adoption of the open source methodology for software development. Today OSI's membership is global and includes the largest and most important open source communities. Funded by membership fees and unconditional donations from diverse open source users and developers, OSI stewards the approval process of open source licenses, seeds education initiatives for all ages, and intervenes to ensure open source is accurately represented both in commerce and in policy.

This document explains OSI's position in relation to the mandate under President Biden's May 2021 Executive Order[2] to secure the software supply chain in defense of cyber-attacks, especially regarding the provenance of its software ingredients (area 5 of the call for papers).

1. With the wider open source community, OSI recognises the importance of the integrity of the supply chain for all software as a vector for compromise and potential attack and welcomes the US government recognition of the issue.

2. Open source licenses provide the rights necessary to use, improve and share software in both source and binary form, *ex ante* and without negotiation, resulting in widespread adoption, reuse and innovation. This software thus has a high profile in discussions of the supply chain, as the majority of the software integrity chains today comprise open source.

3. Open source should continue to be favored in pursuit of supply-chain integrity. The attributes of open source software - especially its ready availability in source-code form and the consequent possibility of experts worldwide applying their skills to maintain and secure it - make it preferable as an ingredient in critical infrastructure because it decouples assurance of integrity from specific relationships with the rights holders.

4. The open source industry has been working on supply chain integrity for a number of years. OSI observes that its Affiliates[3] offer a wealth of expertise, practical experience and open source tools for dealing with SBOM and CI/CD tooling to support it, especially the Linux Foundation[4] and the Eclipse Foundation.[5]

---

[1] https://opensource.org/

[2] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[3] OSI Affiliates, https://opensource.org/affiliates

[4] The Linux Foundation, https://linuxfoundation.org/ who have published a summary of relevant activity at https://www.linuxfoundation.org/en/blog/how-lf-communities-enable-security-measures-required-by-the-us-executive-order-on-cybersecurity/

[5] The Eclipse Foundation, https://www.eclipse.org/org/foundation/

5. OSI further has the following recommendations for specific practices and tools that can be highly beneficial:
    a. That objective mitigations to supply-chain integrity and assurance be adopted in the form of Software Bill of Materials practices, especially performed in compliance with the ISO 5230/OpenChain specifications.
    b. Using the many existing tools for license identification, which ensure that all software components are of known provenance. One example is the Software Package Data Exchange (SPDX),[6] an open standard for communicating information about components, licenses, copyrights, and security references in software, which is expected to become an approved ISO standard later this year.
    c. Ensuring the software in use precisely matches a trusted, canonical build created by the original maintainers or community. One example of this practice is the Reproducible Builds Project[7] which can be used to verify that an executable file is bit-for-bit identical to the original source code it purports to be, thereby detecting any tampering of the downstream supply chain.

6. OSI also notes that these tools and practices are only viable when the full source of each software artifact is available immediately. This can most readily be achieved when the source code in question is available without requiring further permission from or negotiation with the rightsholder, such as code licensed under an OSI-approved license.

7. OSI further notes that the system maintained by OSI-non-profit-Affiliate Software Heritage[8] can deliver precisely-identified source code for a specific version of almost any open source component and recommends that the US government embrace the project, mirror its repository and invest in its evolution.

OSI would be pleased to discuss this position during the NIST Workshop. Please contact:

- Pamela Chestek, Board Member, pamela.chestek@opensource.org
- Simon Phipps, Staff Director of Policy & Standards, simon.phipps@opensource.org, 1 415 683 7660

[6] Software Package Data Exchange Project, https://spdx.dev/
[7] Reproducible Builds Project, https://reproducible-builds.org/
[8] Software Heritage, https://www.softwareheritage.org/