Public Comments for ICR 202311-1670-001

Author Full Name : Moti Gindi **Received Date :** 12/17/2023 10:23 AM

Comments Received :

Section III, clause 2

We suggest to expand clause 2 to cover also risks that are not sourced from vulnerabilities, as following (suggested changes marked in ***):

2) The software producer has made a good-faith effort to maintain trusted source code supply chains by employing automated tools or comparable processes to address the security of internal code and third-party components and manage related vulnerabilities, *** risky material changes and other applicative risks derived from these components ***;

Rationale:
Infiltrated malicious / malware code into first or third party packages (via a multitude of attack vectors) is a source of risk to the produced software, which is parallel to exploitation of vulnerabilities. We suggest therefore emphasizing this.