Public Comments for ICR 202311-1670-001

Author Full Name : Moti Gindi **Received Date :** 12/17/2023 10:20 AM

Comments Received :

Section III, clause 1

We suggest to expand the scope of clause 1 d) to include also maintaining continuous inventory of software components, as following (suggested changes marked in ***):

d) Taking consistent and reasonable steps *** to maintain a continuous inventory of all software components (such as APIs, sensitive data, framework, and dependencies) that makes each environment and its attack surface ***, document, as well as minimize use or inclusion of software products that create undue risk within the environments used to develop and build software;

Rationale:
The ability to immediately report the security posture of each component and the system as a whole is based on continuous understanding of the inventory of these environments, which changes rapidly. Without such ongoing automatic visibility - the software producer is left with blind spots regarding the inclusion of software components and products that affect the attack surface of the overall software. This requirement is aligned with PO.4.2 and PO.5.1 in the SSDF Practices and Tasks.