Public Comments for ICR 202311-1670-001

Author Full Name : Anonymous **Received Date :** 12/08/2023 10:49 AM

Comments Received :

I believe that if the fed government wants to drive vendor behavior (and as the largest procurer of goods and services in the world) it can. The time and money that will be spent by agencies trying to obtain and keep attestation forms in a repository for software obtained as far back as Sept. 14, 2022 is enormous. Attestations are factual, signed statements. Why can't the gov instead ask software producers who can fully attest to using the required secure software practices, post their electronically signed attestations on their websites in a registry much like Microsoft posts Accessibility Conformance Reports online for all of their software? https://www.microsoft.com/en-us/accessibility/conformance-reports

Publicly posted attestations would reduce complexity for Contracting Officers and software producers alike, and improving acquisition should always be the goal. I truly believe that having software producers post their signed attestations on https secure sites will VERY MUCH improve efficiency and save the government and industry money (costs that industry would most likely pass along to the government anyway by raising the cost of their software.)

If 100% of the signed/vouched for attestations were posted on software producers sites, then attestation forms that couldn't yet be signed off on could become in essence, POA&Ms. Software producers who can't post a signed attestation can say to agencies, "we have some known vulnerabilities, let us submit that securely to your agency and we can discuss."

The federal government is already driving behavior by saying that it is going to start collecting attestations. Since M-22-18 was published, I'm sure software producers have been working harder than they had been before to meet NIST guidance. Agencies have huge IT Security and supply chain activities to execute that they may not be fully able to meet if resources are pulled into this complicated attestation collection process. I think the strategies in place to address improve software security are good, but this particular tactic of collecting and storing signed attestations is not the best tactic.

In closing, as software producers move toward using SBOMs and as the proposed FAR rule for software security continues to develop, please keep the end goal in mind. Using the most efficient drivers to ensure that software producers do what they already know must be done to ensure security of the software they produce. Thank you.