Public Comments for ICR 202311-1670-001

Author Full Name : Anonymous **Received Date :** 12/08/2023 04:26 PM

Comments Received :

The Secure Software Self-Attestation Form still contains multiple weaknesses and omissions that, if not addressed, will impose a significant administrative burden on the software producers that submit the form and the Federal Agencies that are required to make informed decisions about the information provided.

The current Form creates the impression that it is applicable to ALL software, ALL at once, except as noted at the bottom of page 2. This problem arises due to incomplete inclusion of all guidance contained in EO 14028. The Form fails to address the issue of “Critical Software” as delineated in EO 14028. HOWEVER, OMB captured this additional guidance in M-21-30 where the emphasis on “Critical Software” was correctly described. M-21-30 further pointed to the obligation of NIST to publish the definition of critical software and a list of software categories and products that are in scope for the definition. NIST did so at Critical Software - Definition & Explanatory Material | NIST. Neither M-21-30 nor the NIST response to the EO 14028 task are included as references and should be.

Furthermore, both the NIST response and M-21-30 define a phased approach to addressing software that will eventually be subject to attestation BUT carefully separates critical software from “other” software. M-21-30 prescribes a schedule for critical software and all other software that has been modified slightly by M-23-16 for critical software.

A second problem is that the presentation of the information that is at the bottom of page 2 and further explained at the top of page 3 has consistently been misinterpreted as readers too quickly jump to conclusions at the end of page 2 before reading the top of page three. In addition, the explanation has been deemed inadequate but was much more elegantly described in M-23-16. Therefore, I highly recommend footnoting the last line on page 2 and the first paragraph on page 3 that points to M-23-16 as a means to advise a reader to refer to the more detailed information that clears up the ambiguity of the Form.