From: [redacted] via 800-171comments
To: 800-171comments@list.nist.gov
Subject: [800-171 Comments] NIST SP 800-171: Comment
Date: Friday, January 26, 2024 4:18:09 PM
Attachments: sp800-171r3-fpd-comment-template.xlsx

Thank you for the opportunity to send comments on NIST SP 800-171 Rev. 3! The attached spreadsheet provides one comment for the forthcoming NIST SP 800-171 update. Thank you!

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
1	Anonymous	Technical	Analysis	51	1846	The most recent draft of the Cybersecurity Framework removed the category addressing "mobile code": DE.CM-05, noting that its concerns are addressed in DE.CM-01 (network monitoring) and DE.CM-09 (hardware, software, and data monitoring). Similarly, NIST SP 800-171 should withdraw 3.13.13, the section addressing mobile code, which is already sufficiently address in 3.14.2, which addresses malicious code protection. The same should be done here, as "mobile code" is a relic-like term from the 90s. Mobile code, as a concept, is a moribund carryover from the days of then-novel "active content" in web browsers in the 90s. Initially, "mobile code" was a label to then-new technologies like Java applets, Flash, Shockwave, and JavaScript. In academia, the study of mobile code remained alive from around 1995 to 2008, but, as happens with most technologies, has since become yet another standard item in the toolbox to the point where it is not addressed as a unique concept. (Indeed, other than JavaScript, all just-mentioned technologies are no longer supported or maintained.) When one was to secure against mobile code back in its heyday, the primary options were to either only run mobile code that was digitally signed or to ensure one's web browser contains sufficient sandbox mechanisms. The code-signing mechanism sounds quaint today: one "picking and choosing" JavaScript to execute today would find an inoperable web, as nearly all webpages use JavaScript and are expected to do so. Regarding sandboxing, 90s-era concerns over poorly sandboxed web browsers have essentially left the discussion thanks to numerous refined security mechanisms created by web browser developers. As an aside, it should be noted that perhaps since NIST last released its final publication on mobile code in 2008, the term "mobile code" has been incorrectly interpreted by nearly everyone as "mobile [device] code." While this is (immensely) understandable, the error is ubiquitous to the point such that nearly no modern publications addressing mobile code do so correctly. (For examples, see [1] NIST SP 1800-48, addressing mobile code as "restrict[ing] [the] upload of file types" on mobile devices; [2] NISTIR 8441, seemingly interpreting mobile code as being related to Hybrid Satellite Networks; [3] NIST SP 800-161r1, discussing mobile code as being about "RFID device applications" and "transport sensor infrastructure"; and [4] NIST SP 1800-1E, interpreting mobile code as addressing electronic health records on mobile devices).	Withdraw 3.13.13, "Mobile Code." In its place, note that its concerns are incorporated into 3.14.2. For alignment purposes, consider taking the same action for SC-18 in NIST SP 800-53.