[redacted] [redacted]

Subject: Comments on NIST Cybersecurity Framework 2.0 and its Implementation Examples from Software Freedom Conservancy

Date: Monday, November 6, 2023 11:09:00 PM

I am writing on behalf of Software Freedom Conservancy, a 501(c)(3) charity focused on the issues of ethical technology and software rights and freedoms for individuals and organizations alike.

We are writing to comment on The NIST Cybersecurity Framework 2.0 (NIST CSWP 29) and its accompanied "Implementation Examples".

We, first of all, thank the drafters on keeping the Framework at a conceptual, rather than granular, level of specificity. Nevertheless, our primary concern is that one key aspect of the supply chain issues, as they relate to Free and Open Source Software (FOSS), may not be adequately addressed in the current draft of the Framework, and this issue has important cybersecurity ramifications.

Currently, nearly all FOSS ultimately deployed in key supply chains often is (by the time it reaches its final deployment) *no longer FOSS*. That occurs for two reasons: (a) the FOSS is licensed under a non-copyleft license, and as such the vendor who incorporates the FOSS has no obligation to provide the software as FOSS to their downstream users (and chooses not to), or (b) the FOSS *is* licensed under a copyleft license (which would require provision of source code and the necessary information to build and reinstall the software), but the vendor is out of compliance with that copyleft license. (Regarding (b): in our extensive (if anecdotal) experience, most deployments of copylefted software in supply chains do not properly meet the source code provisioning requirements of the relevant copyleft license.)

As such, in Section 3.5 (page 24, lines 549 and following) of NIST CSWP 29, we believe it is of particular importance for NIST to educate institutions unfamiliar with FOSS in their supply chain about the complex issues above. The software industry has adopted "open source" as a buzzword, and vendors can easily trick or their customers — what is labeled "open source" often is not. Those customers may legitimately believe that they gain cybersecurity benefits merely because there is some peer-reviewed "open source" in their software stack. But, in fact, their risk might be even worse — since a vendor proprietarized a modified version of that FOSS. Supply chain scenarios further exacerbate this problem, since the vendor behaving badly in this regard could be many times removed from the final deployment.

We therefore strongly recommend that for every organization, as part of the GV and/or ID function, should: "verify that those parts of the supply chain labeled as "open source" truly have provided the required complete, corresponding source code to those components, and that either a third-party (outside of the supply chain), or our own experts, can rebuild and reinstall those components." While we realize this may be too specific to include in the Framework itself, we believe that the quoted text would fit well as an example under GV.SC-05 and/or ID.AM-02 in the "Implementation Examples".

Meanwhile, our organization has extensive experience and expertise in the

issue of FOSS reproducability (i.e., reliably reproducing and verifying that installations of FOSS match the source code release provided). We are interested in working further with NIST on these issues and assist in further drafting of examples and/or offering training on FOSS reproducibility to NIST staff.

We would finally like to make NIST aware that many organizations operating in this area have an excessive focus on the procurement of FOSS technology for incorporation in larger proprietary software solutions in the supply chain. As such, they often encourage solutions that are overly specific, and that do not accomplish the more general goals of auditability, reproducibility and repairabilty that are fundamental to the cybersecurity rationale for FOSS. For example, consider the current industry enthusiasm for software bills of materials (SBOMs): SBOMs are often proposed as comprehensive solutions, but they are quite often simply baroque checklists. Furthermore, complex solutions such as SBOMs are only necessary when software is proprietary; SBOMs value and usefulness for cybersecurity completely evaporates in a pure FOSS environment.

We understand completely that NIST must develop and promulgate recommendations for organizations stuck in the conundrum of cybersecurity challenges found in former-but-now-proprietary FOSS. Nevertheless, we urge NIST to encourage organizations through its recommendations to insist that any software in their supply chain that is ostensibly labeled as “Open Source” can indeed be rebuilt, reinstalled, reproduced and verified by third parties who are outside the supply chain.

Sincerely,
--
Bradley M. Kuhn - he/them
Policy Fellow at Software Freedom Conservancy