TIDELIFT

December 18, 2023

Re: Secure Software Development Attestation Common Form

To whom it may concern:

We write because we think changes between the April and November drafts will significantly reduce the "practical utility" of this form by incorrectly excluding much open source software that is "bundled, integrated, or otherwise used by software purchased by a federal agency" (quoting the NIST Software Supply Chain Security Guidance under EO 14028 Section 4e, henceforth "NIST Guidance") and therefore reducing the "quality [and] utility… of the information to be collected".

This outcome would be significantly inconsistent with both the plain text of the relevant OMB memorandums and with the Executive Branch's overall policy goals, as detailed in EO 14028.

Background

Open source software is critical to the nation's software infrastructure, with various analyses finding that open source is between 70% and 95% of the average software application. Simply put, one cannot secure any software application without also securing the open source contained within.

The NIST Guidance reflects this reality, and M-23-16 follows suit, stating that "minimum … best practices … naturally extend to and guide the utilization of third-party software components, both open-source and proprietary". In other words, in order for the government to be secure, development best practices must extend to *all* software—not just the 5-30% that is proprietary.

Change from April to November drafts

In between the April and November drafts, the scope of the required attestation was changed. In the April draft, open source software obtained *directly by an agency* was excluded, but in the November draft, *any* software that is "freely obtained" is excluded, regardless of who obtained and provisioned the software.

As we will explain, this change is material, and inconsistent with the NIST Guidance, the OMB memos, and the goals of federal policy.

Inconsistency with the NIST Guidance

M-22-18, M-23-16, and the proposed common form are implementations of the NIST Guidance, developed pursuant to EO 14028.

On the question of when open source software is covered, the NIST Guidance is extremely straightforward and explicit. It says (*bold in the original*) that "**[o]pen-source software that is bundled, integrated, or otherwise used by software purchased by a federal agency is in scope.**"

The proposed form's exception for "[s]oftware that is freely obtained and publicly available" directly contradicts this section of the NIST Guidance by accidentally exempting *all* open source, regardless of *who* obtained it. This violates the explicit intent of the NIST Guidance that open source *should* be covered when "bundled, integrated or … used" by "purchased" software.

Inconsistency with language of M-23-16

Pursuant to the NIST Guidance, Sec. A of M-23-16 establishes the baseline that producers of software *must* provide attestations for the software that they provide to agencies.

Sections B.1 and B.2 of M-23-16 are best read not as exceptions to Sec. A allowing attestations to be skipped, but rather as clarifications identifying who can best bear the burden of compliance (and, then if necessary, attestation).

Sec. B.1 ("Third Party Components") makes clear that, where a "producer of software" incorporates third-party software, the burden of compliance and attestation is shifted from the agency to that producer of software. Again, it does *not* say that the burden of compliance and attestation is removed, merely shifted to the vendor. This is consistent with the NIST Guidance that open source used as part of "purchased" software must be consistent with the NIST SSDF.

This is also consistent with the stated purpose of Sec. B.1, which says that best practices "naturally" extend to third-party components. Read in this light, it is clear that the goal of Sec. B.1 is not to exempt *all* third-party components from attestation, but rather that agencies purchasing bundled/integrated software must get an attestation covering the third-party software's compliance *from the seller-provider* rather than one-by-one *from each third-party*.

Read this way, it is clear that Sec. B.1 intends to provide for efficiency by centralizing responsibility with the provider, but does not give the provider (or the agency) a free pass to ignore the important, specifically identified need for compliance and attestation.

Sec. B.2 ("2. Freely Obtained and Publicly Available Proprietary Software") does not contradict this reading of B.1. It exempts agencies from requiring attestations for software *"directly"* obtained at no cost. This makes sense, since agencies "have no opportunity to negotiate with the provider" when software is made available at no cost. This section explicitly does *not* exempt open source *indirectly* obtained, such as through a supplier who themselves uses open source, because in that case the agency has leverage and ability to negotiate provision of compliance and attestation.

RECOMMENDATION: We suggest rewriting the common form's third exception to reflect the language and intent of M-23-16 and the NIST Guidance as: "3. Software that is publicly available *and directly* obtained *by the agency at no cost* ."

Similarly, Sec. B.3 ("Federal Contractor Developed Software") does not exempt agencies from performing best practices. Instead, it says that attestation is unnecessary *because other internal compliance procedures* can "ensure that secure software development practices are followed". Again, consistent with our analysis of Secs. B.1 and B.2, the focus of M-23-16 Sec. B.3 is not exempting people from work—it is merely shifting who must perform the work, and how it must be ensured. The common form's exception should be narrowed in order to make that clear.

RECOMMENDATION: We suggest rewriting the common form's exception as to reflect the language and intent of M-23-16 and the NIST Guidance as: "1. Software developed by Federal agencies, *if the agency has ensured through other means that NIST SSDF practices are followed*."

Impacts on the open source ecosystem

Many participants in the open source ecosystem, including Tidelift in our recent submission to the ONCD's RFI on open source security, and AWS and others in their responses to the first comments on the form, have pointed out that the federal government should avoid placing new burdens directly on open source maintainers. We strongly agree, and our recommended changes to the common form are consistent with this vision.

It is entirely possible for software suppliers to provide attestations for third-party open source software. In response to the NIST Guidance, M-22-18, and M-23-16, the private sector has responded by investing tens of millions of dollars over the last 2 years specifically to innovate and scale up new systems and practices to enable attestation of secure development practices by independent open source software developers. If the proposed revision to the scope of required attestation in the form stands, then that successful innovation will be squandered, the government's policy goals will be subverted, and U.S. citizens will be unduly harmed.

As envisioned by the drafters of the NIST Guidance, M-22-18, and M-23-16, our recommended language would place the burden of compliance on the parties most capable of doing it—large software producers who serve the government on a paid, professional basis. Those parties should, in turn, be able to coordinate supporting open source projects, either by doing the work themselves and contributing it back to the projects, or by paying maintainers to do the necessary security work upstream.

Conclusion

It is important that the intention and clear language of the NIST Guidance be respected by ensuring that the exceptions to the attestation policy do not, as a practical matter, nullify the purpose of the NIST SSDF by excluding 70-95% of software. We respectfully submit that our proposed edits to the exceptions achieve these goals.