December 11, 2023

Cybersecurity and Infrastructure Security Agency Stop 0380
Department of Homeland Security
245 Murray Lane,
Washington, DC 20528-0380

RE: Request for Comment on Secure Software Development Attestation Common Form,
Docket # CISA-2023-0001, Document Number: 2023-25251

Dear CISA,

BlackBerry thanks you for the opportunity to provide input on the second draft of the Secure Software Development Attestation form (henceforward referred to as the "common form"). BlackBerry reviewed the first draft (Document Number: 2023-08823) and submitted a response on June 14, 2023.

BlackBerry appreciates CISA's efforts to advance the common form and notes that several of our concerns were satisfactorily addressed in its second draft. To ensure that self-attestation is as efficient a process as possible for both federal agencies and software producers, we would still recommend, as detailed in our response below, adopting a "Sign once, attest many times" approach.

Below, you will find further comments and questions to the second draft.

1. Software which requires self-attestation

Redundant "and"

The common form is used by software producers to attest that the software they produce was developed in conformity with specified secure software development practices, in particular:

> *The following software requires self-attestation:*
>
> 1. *Software developed after September 14, 2022;*
> 2. *Existing software that is modified by major version changes (e.g., using a semantic versioning schema of Major.Minor.Patch, the software version number goes from 2.5 to 3.0) after September 14, 2022; and*
> 3. *Software to which the producer delivers continuous changes to the software code (such as software-as-a-service products or other products using continuous delivery/continuous deployment).*

We note the "and" at the end of the second bullet, concatenating the conditions expressed by all three bullets. Effectively the concatenation requires submission of a self-attestation when all conditions in each of the three bullets are met.

As worded, no software exists that meets both condition 1 "*Software developed after September 14, 2022*" and condition 2 "*Existing software …*". We recommend that for software to require a self-attestation, the software should meet at least one of the three conditions above. We believe, therefore, that the "and" at the end of the second bullet should be replaced with an "or".

Further guidance for the second condition

We further note that it is at a software producer's discretion to change the version of the software available; the software producer may indicate major changes to the software using just minor version changes, for example. In this case, the software producer could avoid submitting a self-attestation for the updated software.

Additionally, the NTIA recognizes[1] that "a diversity of versioning methods and systems" exists; the semantic versioning schema – identifying the major version concept – is just an example. Software producers using an alternative versioning scheme could avoid submitting a self-attestation for the updated software.

BlackBerry recommends CISA review the conditions in bullet 2 above, ensuring conditions are universally applicable for existing software and leaving no room for interpretation.

2. Individual signing on behalf of the software product(s) or service(s)

The common form restricts the roles of the individual signing the attestation on behalf of the organization to those of the Chief Executive Officer (CEO) or Chief Operating Officer (COO). It should be noted that according to one study, 60% of companies do not have a COO.[2] Companies need not have a CEO either.

Instead of identifying a role (which may not exist in a particular company's organization), it is preferred to identify the signatory based on the responsibilities of that role. For example, an officer signing the common form for a software product or service desired by an agency should be responsible for securing said product or service (e.g. Chief Information Security Officer). BlackBerry recommends that the common form identify the responsibilities of the officer signing on behalf of the software product or service desired by an agency.

3. Provenance

The term "provenance" is limited in meaning by Executive Order (EO) 14028 Subsection 4e(vi), to the origin of software code or components. BlackBerry recommends that CISA clarify whether the location (e.g. URL (Uniform Resource Locator) to a github repository) or the content of the SBOM field "Supplier Name" as defined in NTIA's report "The Minimum Elements For a Software Bill of Materials (SBOM)"[3] would suffice here.

BlackBerry notes that the EU Cyber Resilience Act (CRA)[4] will require "[m]anufacturers to draw up an SBOM", "to be included in the technical documentation and, upon request, to be provided to market surveillance authorities". The CRA has "[n]o requirement to make the SBOM publicly available". Aligning the term "provenance" with emerging practices around the world would be beneficial.

4. Sign once, use many times

Burden

When a software producer opts to sign the self-attestation – as opposed to leveraging a Third Party Assessor Organization – the restriction to limit the designated signee to the Chief Executive Officer

[1] https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf
[2] https://www.mckinsey.com/capabilities/operations/our-insights/stepping-up-what-coos-will-need-to-succeed-in-2023-and-beyond
[3] https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf
[4] https://www.cisa.gov/sites/default/files/2023-09/EU%20Commission%20SBOM%20Work_508c.pdf

(CEO) or the Chief Operating Officer (COO) represents a significant burden. The CEO or COO would need to sign a form each time software or services are sold to an agency, each time a major version change occurs, etc. Involving an officer in each transaction or significant software update is undesirable and expensive.

BlackBerry recommends that a signed form be capable of reuse when other agencies procure the product (for the same major version of the software or service).

Agency-specific instructions

BlackBerry recommends that agency-specific instructions – applicable to either the common form or its submission process – be minimized, and preferably avoided altogether. Ideally, the number of times an organization will need to sign a common form will be minimized and the signed form can be reused when other agencies procure the software. Agency-specific instructions, including an agency-specific "submit" button in the PDF, or specific e-mail instructions (e.g.for assuring confidentiality, integrity of the e-mail), may hamper the ability of the software producer to sign what is essentially the same attestation only once.

Recommendation

Therefore, BlackBerry recommends that:

- the common form be common across agencies and need only to be signed once for a product of a particular release or a product line. (The software producer can maintain a repository with signed attestations and reuse them, if applicable);
- the submission procedures be unified yet secure, preventing unnecessary differences and preventing submission of common forms that have been spoofed or tampered with; and
- the effort to create a single, US Government-wide repository for received common forms be prioritized, as having a single repository reduces duplication of effort for software producers and agencies alike.

5. Conclusion

In summary, BlackBerry strongly supports CISA's effort to implement Software Supply Chain Security Guidance under EO 14028 in consultation with the private sector. We appreciate the opportunity to offer our input. Mr. John-Luc Bakker (JBakker@BlackBerry.com) is available to respond to any questions you may have concerning BlackBerry's views.

Respectfully submitted,

J.H.L. Bakker

John-Luc Bakker
Director, Standards