BlackBerry

June 17, 2021

National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, NW
Washington, DC 20230

Re: Software Bill of Materials Elements and Considerations [Docket No. 210527-0117]

Dear NTIA,

BlackBerry Corporation[1] respectfully submits these comments in response to the National Telecommunications and Information Administration's (NTIA) request for comment on the minimum elements of a Software Bill of Materials (SBOM), pursuant to Executive Order (EO) 14028 on Improving the Nation's Cybersecurity. BlackBerry shares NTIA's long-standing concern over security vulnerabilities in the software supply chain, which is vital to the Federal Government's ability to perform its critical functions, and applauds the efforts and foresight reflected in the recent EO 14028 to bring greater transparency to the supply chain and ensure that software products function securely and as intended. We stand ready to support NTIA, and the Federal Government more broadly, in taking the critical steps necessary to rapidly improve the security and integrity of the software supply chain.

General comments

BlackBerry commends NTIA's leadership in advancing software supply chain transparency and in its utilization of an open and consensus-based multi-stakeholder process on this topic. We support our nation's initiatives to secure the software supply chain through use of SBOMs and agree that widely used, machine-readable SBOMs when coupled with automation and tool integration will bring significant benefits in securing federal agencies and the nation's IT and OT systems.

We observe that what constitutes the *minimum* viable elements of SBOM is very much dependent on what the *goal* is. We interpret the current goal as achieving the best possible cybersecurity of the software supply chain through utilization, to the maximum reasonable extent, of technology that is widely available today. To that end, given that Software Composition Analysis (SCA) tools already exist to automate the production and verification of information about software components, and can be used by both primary and secondary (non-

[1] BlackBerry Corporation has provided secure communications to the world's governments and largest businesses for over 35 years. From secure devices, we have shifted to building some of the world's most advanced cybersecurity technologies, utilizing Artificial Intelligence (AI) and Machine Learning (ML) to ensure zero-trust environments for some of the most critical operations. This, combined with BlackBerry's work on secure real-time operating systems that power everything from 175 million vehicles worldwide to vital observation equipment on the International Space Station, places our company in a unique position as a software provider offering operational effectiveness with security built into the very design of our products and services.

BlackBerry Corporation
3001 Bishop Drive, Suite 400, San Ramon, California, 94583 USA. tel: +1 (925) 242-5660 fax: +1 (925) 242-5661

supplier) SBOM authors, the information generated by such tools should be combined with any other information that is available to the SBOM author such that every reasonable effort has been made to ensure that the bill of materials is complete and without omissions.

Given the current state of practice, when it comes to defining the minimum elements of SBOM it is important to ensure that secondary SBOM authors can satisfy the requirements to provide the minimum set of elements in case no authoritative or reliable SBOM of subcomponents is available. Often, secondary SBOM authors only have access to binary images and are therefore reliant on binary scanning.

We suggest that support be provided for viewing the SBOM from the perspective of the constituent files that comprise the software in addition to providing support for viewing the components. The meaning of 'file' is well understood and is something that can be referred to by both primary (supplier) SBOM authors as well as secondary SBOM authors, the latter of which may be reliant on binary scanning tools.

We also believe that the concept of using hash as an identifier is more applicable from a file-centric viewpoint, because files provide a concrete target on which to generate a hash as well as to re-calculate the hash for verification purposes. Enabling support for viewing SBOM from the perspective of the file also facilitates documentation of artifacts beyond source and binary code, such as config files, shell scripts, etc., which can also have a critical bearing on the cybersecurity posture of a software product.

Since a file may contain multiple components (e.g. different OSS libraries) we suggest that more clarity is needed regarding the definition of 'Cybersecurity hash of component' and 'Any other unique identifier', since these could potentially present problems for binary scanning tools depending on how they are intended to be generated and used. Based on our understanding of the intended use cases, we would recommend that these elements should be made optional.

Response to NTIA RFC questions

Question 1: Data fields and operational considerations

We suggest that it should be possible to perform a vulnerability look-up using a software identity that is derived from a sequence of information that includes supplier name, component name and version. Hence, we agree that these 3 elements (supplier name, component name and component version) should be included in the minimum elements of the SBOM.

Question 3.c: Legacy and binary-only software

We propose that software suppliers or secondary SBOM authors should be required to provide as much information as possible in the SBOMs of such legacy software, whilst also being able to indicate "unknown" against any of the elements in the minimum list of elements (similar to the NTIA's proposed operational consideration regarding SBOM depth). Further details and rationale are provided in Note 1 of the Annex.

BlackBerry Corporation
3001 Bishop Drive, Suite 400, San Ramon, California, 94583 USA. tel: +1 (925) 242-5660 fax: +1 (925) 242-5661

Question 3.d: Integrity and authenticity

Establishing integrity and authenticity of an SBOM is important given its intended use in identifying and mitigating vulnerabilities. If an SBOM can be manipulated by malicious parties then the ability to defend and secure the product can be negatively impacted.

In order to support the ability to pass an SBOM along a supply chain that may encompass heterogenous developer ecosystems, it is desirable for SBOM authors to be able to optionally associate a cryptographic signature with each SBOM. Given the importance of protecting federal systems, BlackBerry recommends that a PKI-based solution be used, wherein the authenticity of the SBOM author can be vouched for by a Certificate Authority (CA).

Question 3.i: Vulnerabilities

We agree that the awareness of and status of vulnerabilities may change over time, and therefore vulnerability information should not be included in an SBOM. The minimum elements of SBOM should be defined such that the information provided supports the use of automated tooling to search vulnerability databases to identify any potential vulnerabilities.

Question 4: Implementation issues for certain elements

We do foresee some difficulties in providing some of the proposed minimum elements in the case where the (secondary) SBOM author differs from the software supplier. Specifically, in the case where a supplier or end customer (acting in the role of SBOM author) only has access to the binary of one or more components provided by upstream suppliers, and/or where SBOM authorship through binary analysis is preferred over the alternative of source code-based static analysis. This is elaborated upon in the following points.

<u>Regarding 'Cybersecurity hash of the component'</u>

We believe that hash of software components should not be a mandatory minimum element of an SBOM. One reason is that production of the hash of a component will not always be possible in the case of secondary SBOM authorship, for example when binary analysis is used to produce the SBOM and the code being analyzed has been statically linked.

We suggest that NTIA should clarify the intended purpose of the hash. BlackBerry can foresee a few potential use cases or benefits, but we do not believe that the use cases need to be mandatorily supported (further discussion is provided in Note 2 of the Annex).

We request that NTIA should further clarify the method for creating the hash (who, when, what, how), and in particular whether the hash can or should be derived from binary or source. BlackBerry believes that if (e.g. optional) support for a hash is to be provided, then making a hash over the binary should be at least one of the options (further details and rationale is provided in Note 3 of the Annex). If hash is to be used in verification by the end consumer or a downstream supplier then the SBOM should also include a description of how to re-generate the hash.

BlackBerry Corporation
3001 Bishop Drive, Suite 400, San Ramon, California, 94583 USA. tel: +1 (925) 242-5660 fax: +1 (925) 242-5661

Regarding ‘Any other unique identifier’

In a similar vein to our comments on hash, we suggest that NTIA should clarify what the intended purpose is of the ‘Any other unique identifier’ element. Without knowing the intended purpose and use it is possible that this element could present a problem for the case of secondary SBOM authorship using a binary scanner.

We foresee potential value in this element for the SBOM creator, for example to distinguish between duplicate instances of the same component (supplier/component name/version), where the ability to distinguish between duplicates cannot be achieved through use of ‘Dependency Relationship’. However, for this use case, given that alternative solutions will sometimes exist to distinguish components, we would suggest that this element should be optional.

We observe that in the NTIA multi-stakeholder community documentation, one of the proposed methods is to use a Type 5 UUID (hash over name space and name), and in this instance we are not clear on how this would fulfil the use case of distinguishing between duplicate instances of the same component.

Conclusion

To conclude, BlackBerry is supportive of the initiative to drive wider adoption of SBOM and associated development of automated and integrated tools to enhance security of the software supply chain. We thank NTIA for the opportunity to provide comments on the notice, ‘Software Bill of Materials Elements and Considerations’. We offer Mr. Takashi Suzuki, tsuzuki@blackberry.com to address any questions.

Respectfully submitted,

Stephen Barrett

Stephen Barrett,

Director, Standards

Takashi Suzuki

Takashi Suzuki

Senior director, Standards

BlackBerry Corporation
3001 Bishop Drive, Suite 400, San Ramon, California, 94583 USA. tel: +1 (925) 242-5660 fax: +1 (925) 242-5661

Annex

Note 1: Rationale for wider support of 'known unknowns'

It seems highly likely that there will be many instances of legacy/binary-only software being used across U.S. government agencies. Replacing or updating this software and these services will take time. The EO indicates in section 4(q) that legacy products already procured by agencies will either need to comply with the requirements of the EO or the agency will be required to put remediation plans in place. We note that especially in the case of proprietary (non OSS) software it may not be possible for a scanning tool to determine information such as supplier, component name and version. Hence, we suggest that vendors (or secondary SBOM authors) should be required to provide as much information as possible for the SBOMs of such legacy products using any information they may still have about the product, while for each minimum element of SBOM, being able to indicate "unknown" similarly to the NTIA's proposed operational consideration regarding SBOM depth. This will allow federal agencies to make an informed decision regarding accepting the risk of continuing to use the legacy software or find an alternate solution. It will also enable clear visibility of where there are information gaps, such that steps can be identified to try and address those gaps.

Even partial information can have cybersecurity benefits. For example, a secondary SBOM author may be able to identify supplier and component name but not version number. This partial information can still be of use in providing a notification to, for example, an end consumer that a CVE exists against a version of the same product (even though it is unknown whether the CVE is applicable for the particular version of the product that the end consumer is using).

Note 2: Purpose of the hash

A hash can be used to bind a precisely defined (e.g. bit-level accurate) description of a software component, or software artifact, to a particular SBOM. The information could enable identification of the situation where the same software artifact has been given different supplier/component/version names, and similarly identification of the situation where the same supplier/component/version information has been assigned to different software artifacts. These capabilities might, for example, be useful during a security incident investigation. Alternatively, it could provide a method for a supplier or consumer to verify that their multi-component software artifact does indeed include the component referenced by an upstream SBOM. In our opinion, all the use cases have value, but support for them should not be made essential.

Note 3: Method for creating a hash

If a hash is to be included as one of the minimum elements of an SBOM (e.g. optionally) then support for providing a hash of the binary should be provided.

BlackBerry Corporation
3001 Bishop Drive, Suite 400, San Ramon, California, 94583 USA. tel: +1 (925) 242-5660 fax: +1 (925) 242-5661

A hash of the binary can have advantages over a hash of the source, for the following reasons:

1) Source code is not always available to the SBOM author. This is especially true the further downstream in the supply chain that SBOM authorship occurs.
2) From a security standpoint, which is the main concern of the EO, the binary (as opposed to source) is the definitive artifact of interest for identifying and determining vulnerability of deployed software.
3) A hash of a binary will sometimes already have been created by a supplier when generating a cryptographic signature of a deliverable that is being provided to a downstream supplier or consumer.

We observe that a hash of the binary of the complete software image can always be provided by a secondary SBOM author, however, it may not always be possible to obtain a hash of components (e.g. where static linking has been used).

BlackBerry Corporation
3001 Bishop Drive, Suite 400, San Ramon, California, 94583 USA. tel: +1 (925) 242-5660 fax: +1 (925) 242-5661