PUBLIC SUBMISSION

As of: June 19, 2021
Received: June 15, 2021
Status: Pending_Post
Tracking No. kpy-if4y-gzom
Comments Due: June 17, 2021
Submission Type: Web

Docket: NTIA-2021-0001
Software Bill of Materials Elements and Considerations

Comment On: NTIA-2021-0001-0001
Software Bill of Materials Elements and Considerations

Document: NTIA-2021-0001-DRAFT-0003
Comment on FR Doc # 2021-11592

Submitter Information

Email: vidya@medcrypt.com
Organization: MedCrypt

General Comment

To successfully implement an SBOM management lifecycle that spans technology, people and processes, there are several attributes that must be realized for it to be practically usable, executable and scalable and for meaningful progress to be made. This includes an established convention and agreement on:

-usable format for consumers, including machine readable, standard formatting & fields, enabling further analytics
-standardized formatting of supplier and component names
-security-relevant versioning of components including accurately reflecting patch level/type, and
-consideration around assurance of SBOM integrity via cryptographic hash

Furthermore, to encourage the adoption of an SBOM for business operations, it is possible to consider applying for license tracking & management, component end of life management as well as export control.

While the EO has the intention and spirit we align around, healthcare has learned in the implementation of HIPAA that taking a reactive stance, blaming end users and waiting for perfect will result in never moving the needle.