May 30, 2021

INCD Position Paper on Notice and Request for Comments on Software Bill of Materials Elements and Considerations

The Israeli National Cyber Directorate wishes to present this position paper re relevant Notice and Request for Comments on Software Bill of Materials (SBOM) Elements and Considerations.

1. Assuring compatibility with common standards – It is highly recommended to assure SBOM compatibility with common standards recommendations, such as ISO/IEC 5320:2020 - Information technology — OpenChain Specification and SBOM document format options (e.g. SPDX, SWID, and CycloneDX).

2. Minimum elements for an SBOM:

א. Supplier Name
ב. Component Name
ג. Unique Identifier
ד. Version String
ה. Component Hash, Metadata and File Entropy Level
ו. Relationship and Dependency
ז. Author Name
ח. Licenses
ט. Vulnerabilities
י. Source and Package repos
יא. End to Sale (EOS) date
יב. End of life (EOL) date
יג. Common Attack Pattern Enumeration and Classification (CAPEC) that can be used to attack the component

3. Operational considerations –

יד. Frequency - Each new component version should include its own SBOM, while providing a track change\version diff.
טו. Depth – It is recommended to provide a full tractability capability and not only dependencies mapping.
טז. Delivery – The SBOM should be published to the public by each vendor and should be consolidated to a central public database (like NVD). In addition, SBOM should be supported by common information sharing protocols such STIX/TAXII.
יז. Automation support – The end user should obtain a full automation capability so the time and effort using the SBOM would be minimized. For instance, each integrated development

environment (IDE) tool should provide to the developer a real time report on the code authenticity level and further information on the SBOM itself. The SBOM should be enforced by common Application Control tools such as Microsoft AppLocker. Re the last example, the Source Control Management (SCM) tools should allow the Cyber team to compare the code to the SBOM before initiating an import process to the repository and to rerun this test according to predefined schedule. In case that the code doesn't fit to the SBOM, a real time alert should be sent to the Cyber team.

INCD would be glad to join the relevant working groups on those issues. This paper was written by Mr. Yuval Sinay.
For further inquiries, please contact Ms. Gali Levakov, INCD Attache to the Israeli Embassy, Washington DC at Glevakov@cyber.gov.il