NIST,

Thank you for providing a final opportunity to participate in this important work.

**In the area of Description:**

Naming the software provider entry should have the ability to maintain the history of the product. Companies and products may change hands. It is important to know the basis of the product. What company developed the software? Are they utilizing a generic email account, [e.g., security@company.com], for the intake of questions or reports?

Naming the software identifiers should be complete. (Is this area intended to be the SBoM?) Today it makes sense to maintain the history of the product, therefore this area of the labeling should be updateable. Is the source code still available for updating? What libraries were included?

Declaring a manufacturer or vendor (company) has a vulnerability reporting program or mechanism suggests a binary response: yes or no. Judging the capability and maturity of a vulnerability reporting program requires more information. Asking if the company is a CVE Numbering Authority or has requested CVEs from MITRE to identify vulnerabilities in their products provides much more information.

**In the area of Critical Cyber Security**:

Declaring a product is free from known vulnerabilities suggests a binary response: yes or no. What would be useful is a date of last update, a CVE identification number, or a software version number. This level of detail would provide a starting place for the customer to begin researching what remediation or mitigations can be expected to be already included in the product.

Authentication and authorization is often assumed to be the same. Please ensure the multifactor authentication and use of strong cryptography don't become the end result. Knowing when and where to implement them is key. Device A is authenticated to Device B, but is Device A authorized to make changes to Device B?

Please have a safe and happy holiday.

Best regards,

Laurie Tyzenhaus