From:	Caleb Queern <cqueern@gmail.com>
Sent:	Tuesday, June 1, 2021 12:43 AM
To:	SBOM_RFC
Cc:	Friedman, Allan
Subject:	Request for Comments on Software Bill of Materials Elements and Considerations

To Whom It May Concern,

NTIA is requesting comments on the minimum elements for an SBOM. I understand that the current "baseline component information" includes:

- Supplier name
- Component name
- Version of the component
- Cryptographic hash of the component
- Any other unique identifier
- Dependency relationship
- Author of the SBOM data

Recommendation 1 of 2: I recommend that NTIA consider elements found in the emerging security.txt standard for use in SBOMs. The latest draft of the security.txt standard as of this writing may be found at:

https://datatracker.ietf.org/doc/html/draft-foudil-securitytxt-12

Elements found in the security.txt standard which may be useful in SBOMs include:

- Contact
    - Security.txt usage: A link or e-mail address to contact an organization about security issues
    - Potential SBOM usage: A link or e-mail address to contact the SBOM author about security issues
- Policy
    - Security.txt usage: A link to a policy detailing how security researchers should report security issues
    - Potential SBOM usage: A link to a policy detailing how security researchers should report security issues

Recommendation 2 of 2: I recommend that NTIA consider explicitly declaring each SBOM element as "required" OR "optional". This designation would apply to the baseline component information as well as any new SBOM elements that are adopted.

Thank you,
Caleb Queern