Use cases for SBoMs in Energy

- There are many use cases for SBoMs. There are uses for software suppliers, as well as for organizations that use software.
- I recommend you read the excellent document “Roles and Benefits for SBoM across the Supply Chain”, available at https://www.ntia.doc.gov/SBOM
- I want to focus on what I consider the three most important use cases for SBoMs for electric power industry organizations. However, when the Proof of Concept starts, it will be up to the participants to decide which use case(s) they wish to focus on in the PoC.

A. Vulnerability management

- The average software product contains many components, both proprietary and open source.
- To manage vulnerabilities, you often enter the name of a software package in the National Vulnerability Database (NVD), to identify vulnerabilities (CVEs) that apply to it. Or simply scan the software with Nessus or a similar product.
- But few Energy organizations try to manage vulnerabilities in *components* of a software product. Without an SBoM for the product, they don't even know what those components are. The NVD doesn't know what components are in any software
- With SBoMs, your organization can track and mitigate vulnerabilities in components of software you own, as well as vulnerabilities in the "first party" code itself.

B. Procurement

- When you're procuring software, you should learn about vulnerabilities found in the products you're considering.
- If you just look at the CVEs that apply to the product, you're probably missing a lot more CVEs that apply to the components. You won't know about these without an SBoM.
- If you know about open vulnerabilities in components, you can require in the contract that they be patched or otherwise mitigated before the purchase is complete.
- More generally, you can require terms for how the supplier will address component vulnerabilities going forward. And you can require that they update their SBoM whenever there are changes in the components.

C. The Ripple 20 syndrome

- How many of you had to respond to the Ripple 20 vulnerabilities? Those were serious vulnerabilities in a component (an IP stack) from Treck, a company in Cincinnati. They were estimated to affect hundreds of millions of products worldwide.
- If you had a list of every software or hardware product on your network that was affected by Ripple 20, your job would have been much easier. But you would need SBoMs in order to have that list.
- I won't promise that SBoMs will ever give you a list of *every* product that contains a particular component. But I promise you'll be much better off with SBoMs than without them.
- More specifically, SBoMs aren't an all-or-nothing proposition. You are better off with just a partial SBoM for one product than with no SBoM at all. The more SBoMs you have, and the more complete they are, the better off you'll be.

No regulations!

- In a highly regulated industry like Energy, you might think the Proof of Concept will produce standards, guidelines, best practices, etc. – for production and use of SBoMs.
- That's not what NTIA does. They try to promote use of important new technologies by the private sector. You can't regulate a new technology into existence.
- What's needed is informal agreement by a critical mass of software suppliers and users on how SBoMs will be produced and consumed. The best way to do this is by industry. First came Healthcare, then Autos (both ongoing). Now it's Energy's turn.

An example: DNS

- One of NTIA's most important successes was DNS. While they didn't develop the concept, they established the structure for administering DNS.
- In the 1990s, NTIA turned this job over to the IANA, which runs DNS today – with a budget of around $100 million.
- Nobody is required to use DNS. If you have a web site, you can always give out your IP v6 address to anyone who wants to access your site, so they don't need to use DNS at all.
- Of course, you might have to tell them the address by phone, because sending it in an email requires use of DNS!
- You get the idea: DNS exists because users and producers of web content have agreed that it's an efficient, effective solution. There's no regulation behind it. The same will be true of SBoMs.