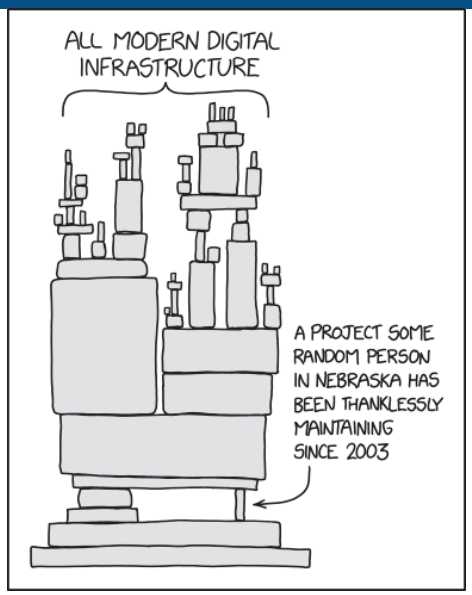
SBOM & Securing the Software Supply Chain:
Progress & Future Directions

Justin Murphy
Vulnerability Analyst
Cybersecurity & Infrastructure Security Agency

Will this be worth my time?

- The case for transparency
- What is an SBOM?
- Why aren't we doing this today?
- What we've done so far
- EO 14028 & "Minimum Elements"
- Gaps: what we're still working on
- Future directions



https://xkcd.com/2347/

TL;DR

1. SBOM is Coming.
2. There is no reason organizations cannot use SBOM today, but we cannot assume universal full automation and integration.
3. Further work is ongoing to scale and operationalize supply chain transparency.

Cliches to avoid in Cybersecurity

Silver

Bullet for

Omniscient Risk

Management

Transparency can help markets thrive

- Food ingredients and food labels
- Safety Data Sheets in the chemical industry
- Hardware Bills of Material (BOM) in industry
- Naming and tracking components can can drive innovation (e.g. CVE)

"Know what you have"

Title search: SBOM and Securing the Software Supply Chain: Progress & Future Directions

Also available as part of the eCourse
2022 Technology Law eConference

First appeared as part of the conference materials for the
35th Annual Technology Law Conference session
"SBOM and Securing the Software Supply Chain"