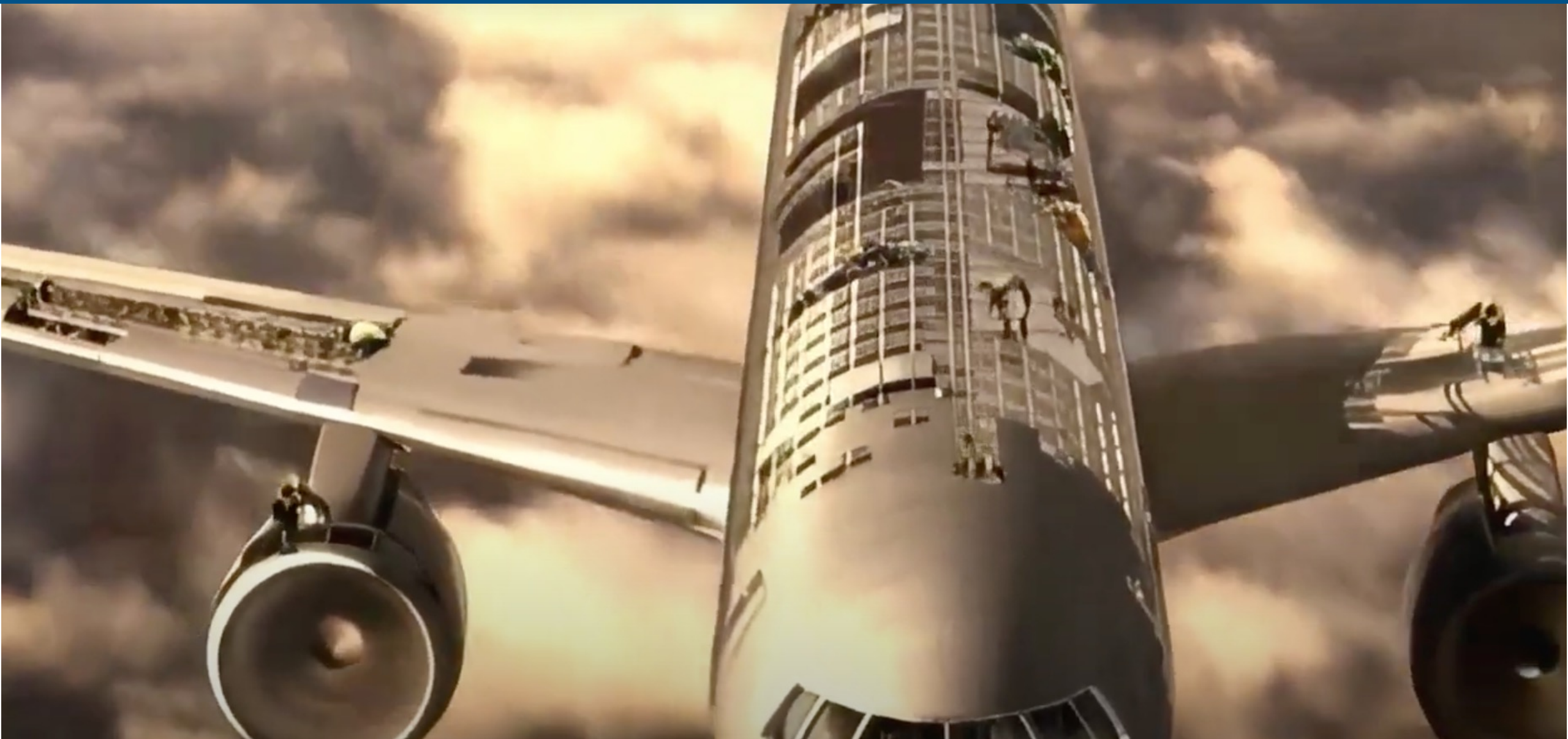
SBOM AND SECURITY TRANSPARENCY HOW IT ALL FITS TOGETHER

Allan Friedman, PhD
“The SBOM Guy”

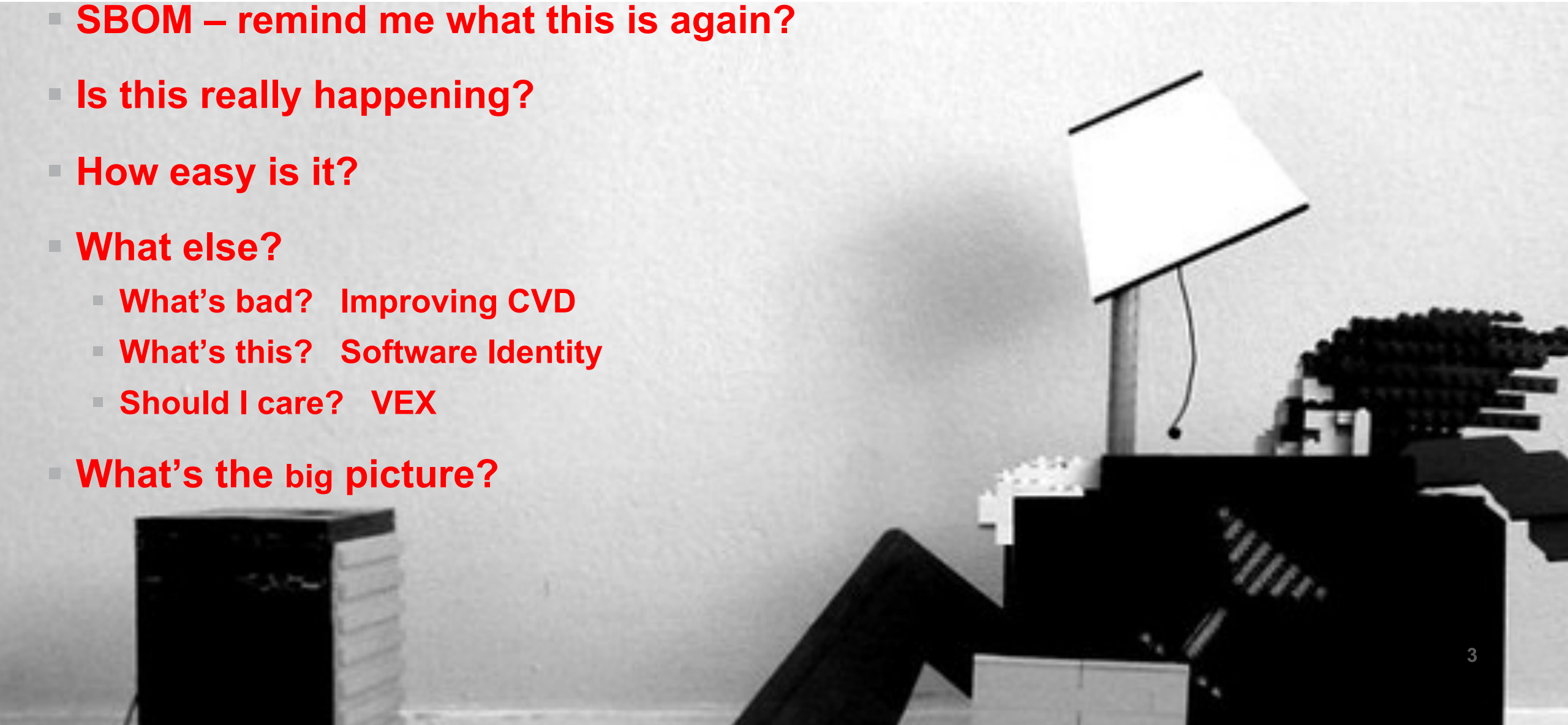
Allan.Friedman@cisa.dhs.gov
14 November, 2024

“Building the Plane While Flying It”



Overview (Why should I watch a video?)

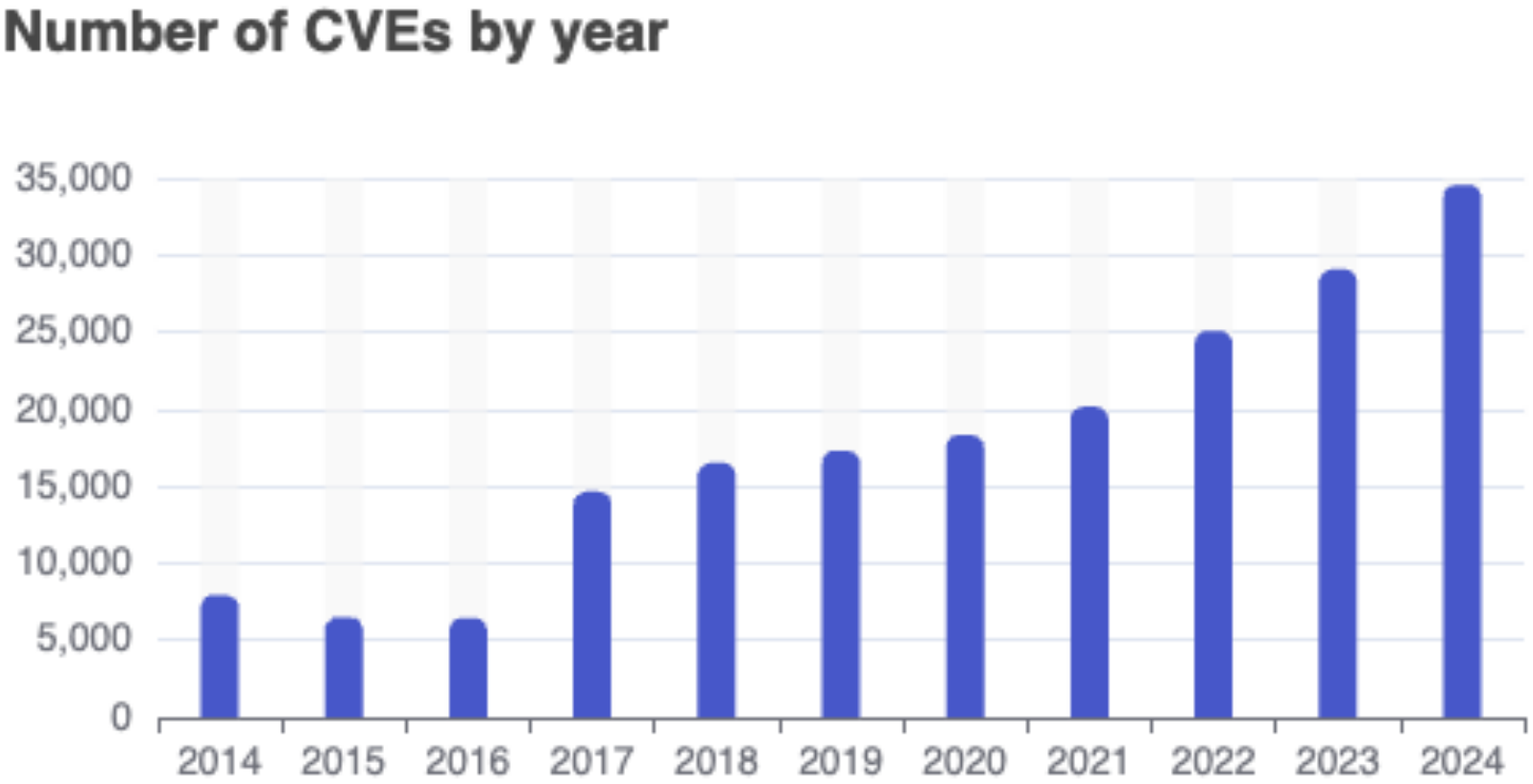
- SBOM – remind me what this is again?
- Is this really happening?
- How easy is it?
- What else?
  - What's bad? Improving CVD
  - What's this? Software Identity
  - Should I care? VEX
- What's the big picture?




CISA
SBOM
CISA.GOV/SBOM

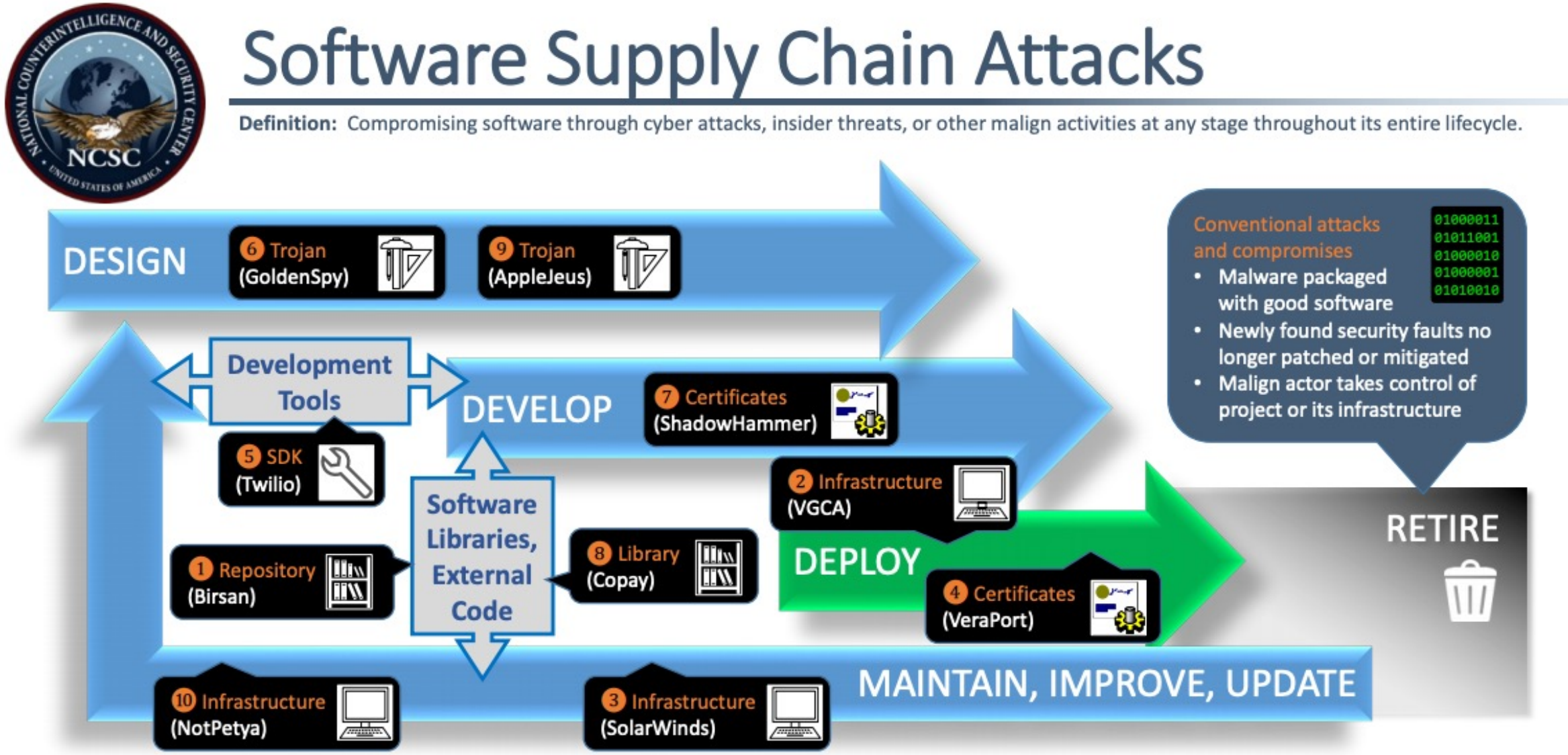
The “new normal” of risk

- Picture c



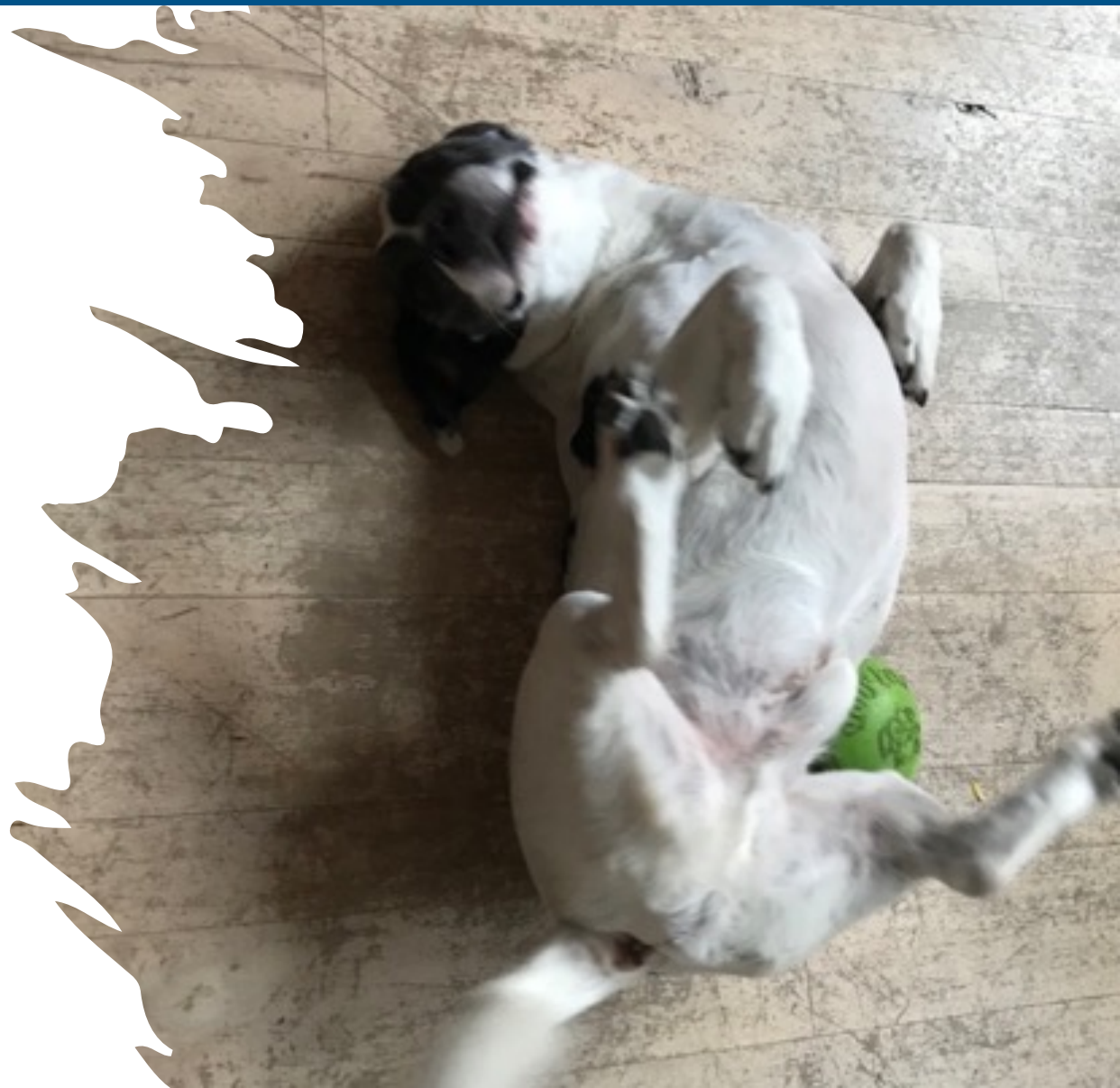
Allan.Friedman@cisa.dhs.gov
14 November, 2024

The “new normal” of risk



Supply chain attacks as the “belly” of security

- Traditionally not as well defended
- Usually an internal issue
- We forget that it is exposed



Types of supply chain risks

- Vulnerabilities
- Intentional malicious insertions upstream
- End-of-life and end-of support code
- Cloned or backdoored versions
- Modified source code
- Risk from open source maintainers
- Midstream compromise – bad updates
- Internal code reuse

Solution: transparency

Transparency can help markets thrive

Transparency can help markets thrive

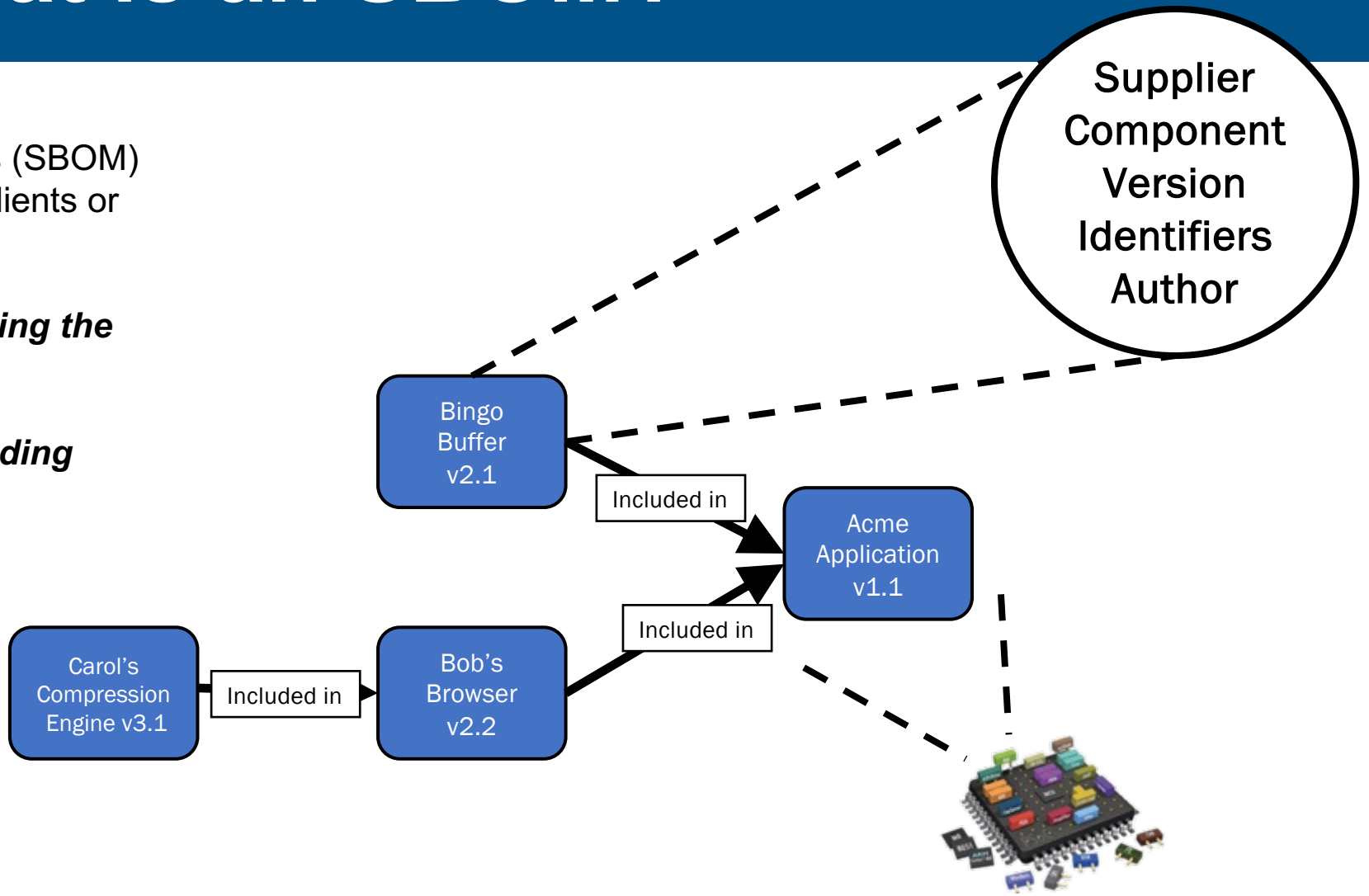
Software Transparency won't solve all our supply chain concerns, but it is necessary component of any scalable solution.

So… what is an SBOM?

A Software Bill of Materials (SBOM) is effectively a list of ingredients or a nested inventory.

"A formal record containing the details and supply chain relationships of various components used in building software"

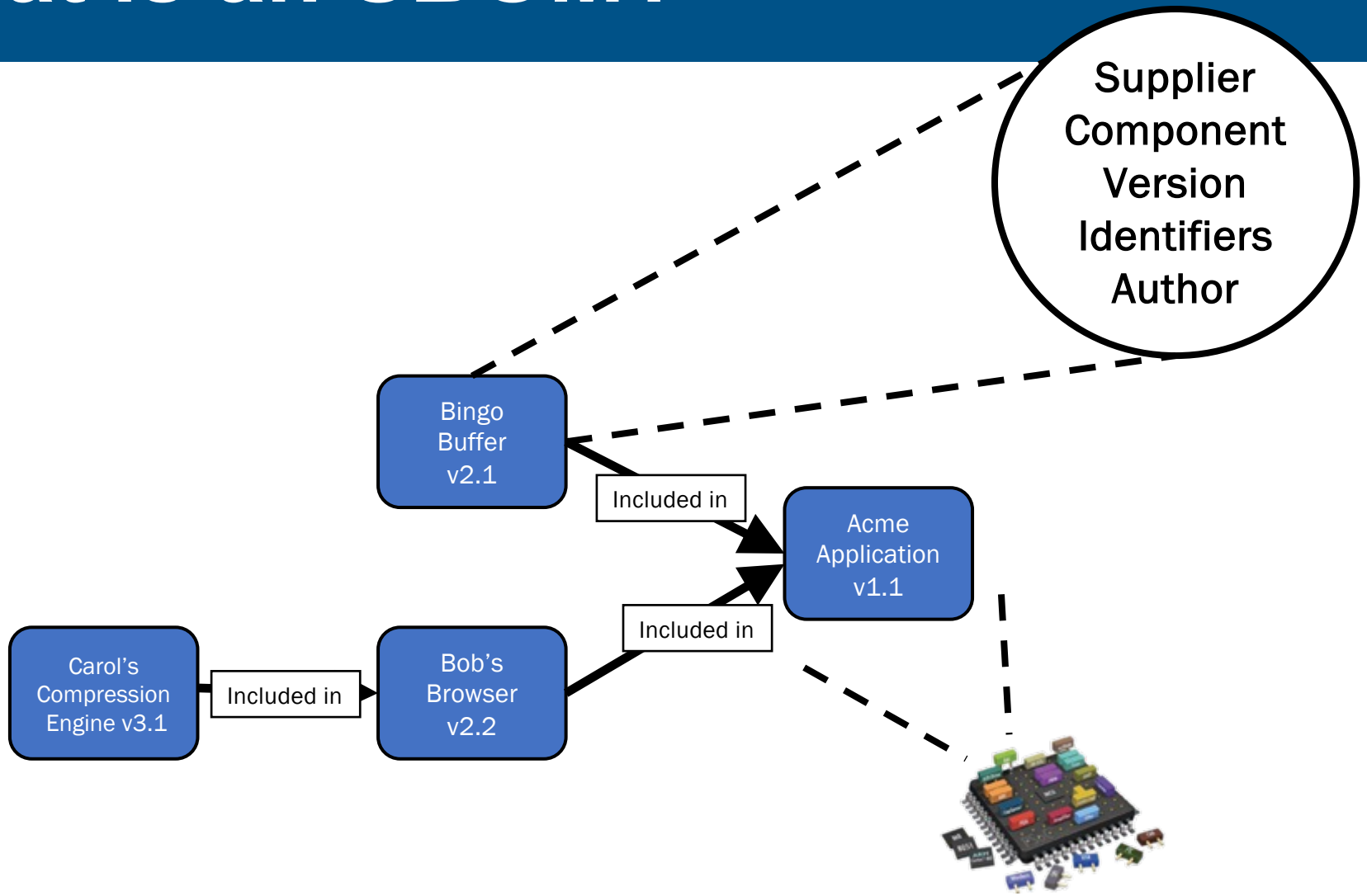
.



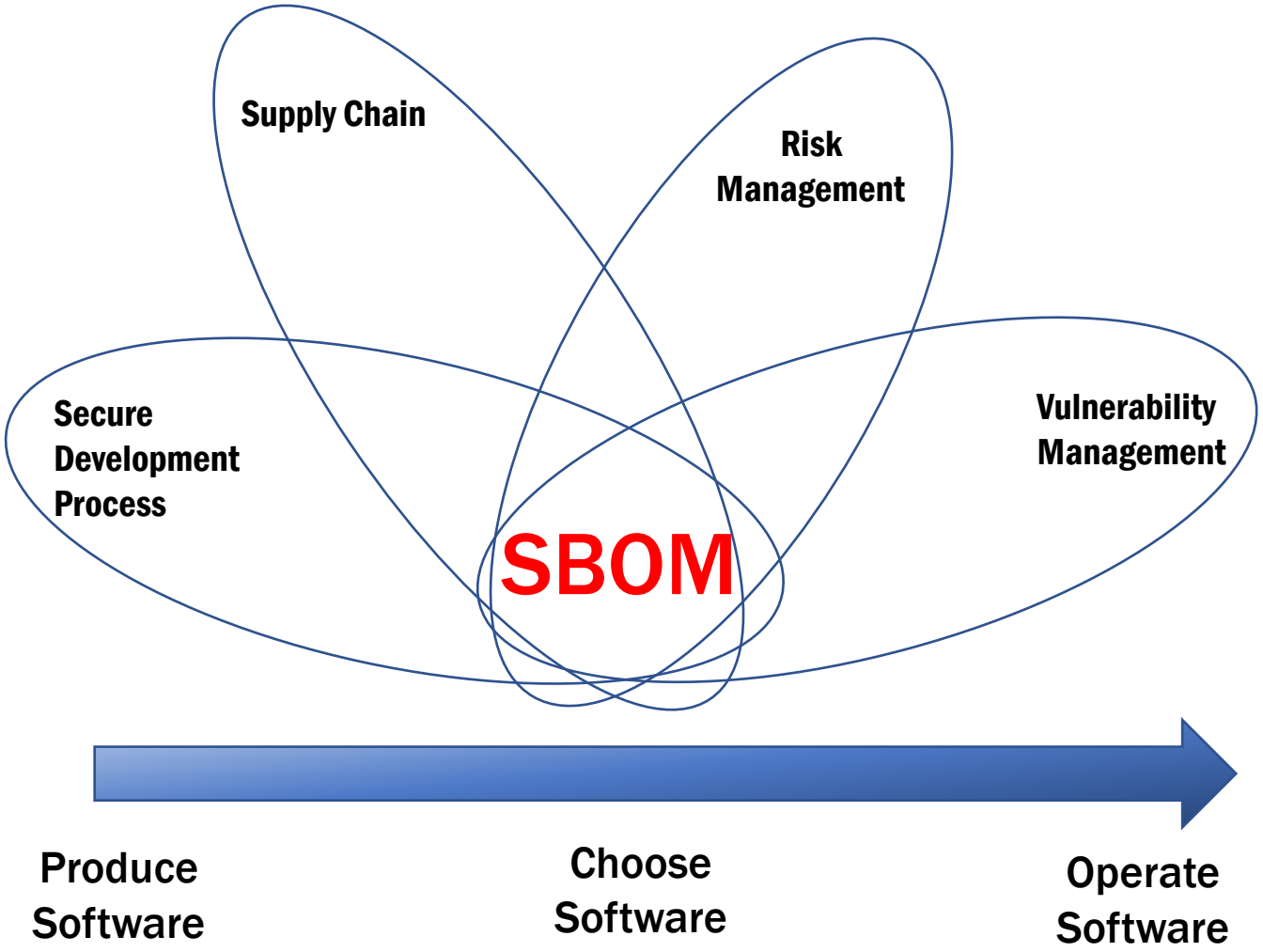
Allan.Friedman@cisa.dhs.gov
14 November, 2024

So… what is an SBOM?

- Proprietary Software
- In-house Modules
- Open Source Code
- Contractor Software
- Built Binaries



Value across roles



Allan.Friedman@cisa.dhs.gov

Regulation and Compliance are coming

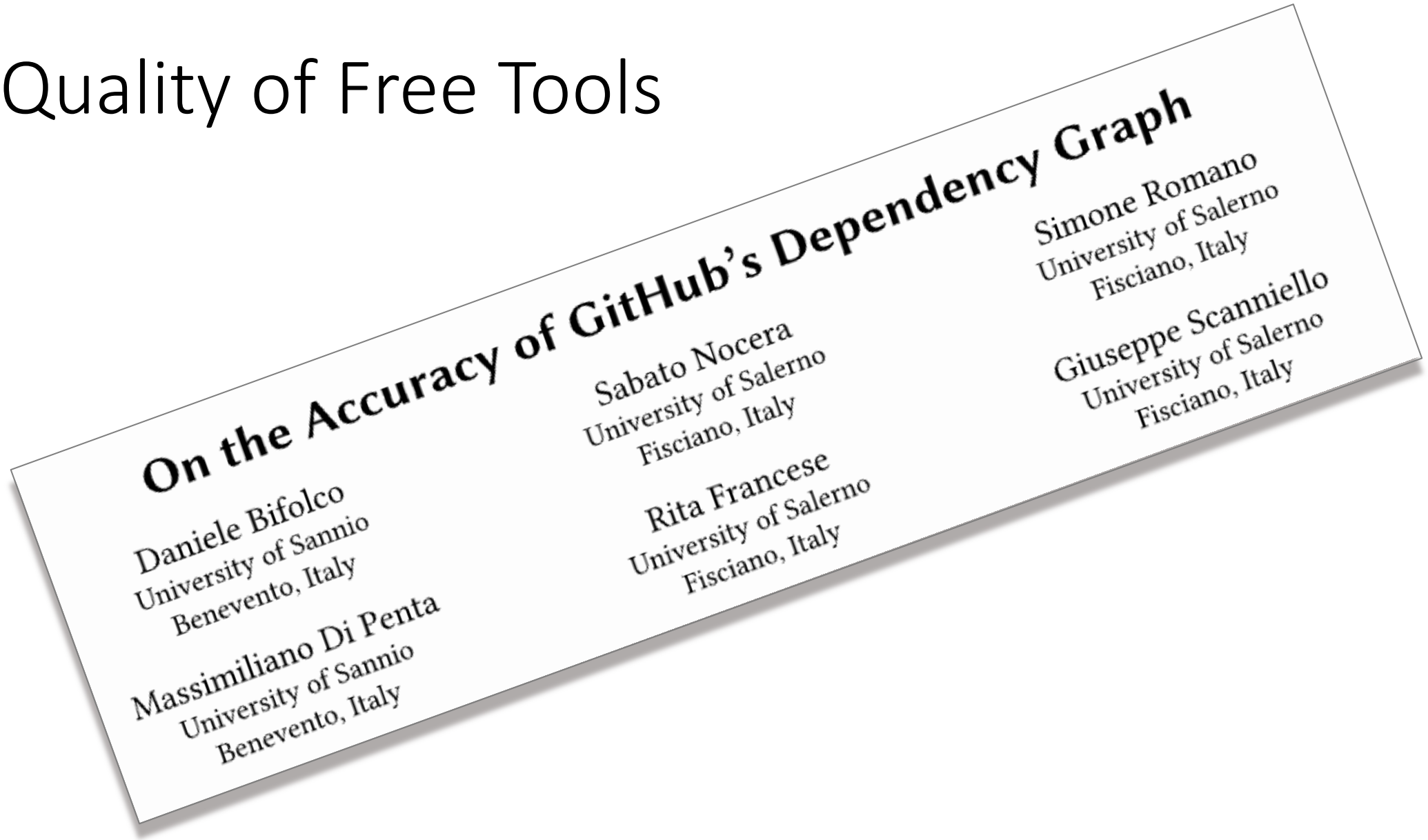
SBOM in Regulations and Guidance Around the World

- US Executive Order 14028
- US FDA Medical Device Requirements
- US BIS Connected Vehicles
- US Army
- Indian Securities and Exchange Board
- CERT-In Technical Guidance
- Japan METI Guide
- German BSI TR-03183
- PCI DSS 4.0
- EU DORA
- **EU Cyber Resilience Act**

Data quality

- Risk: poor quality or immature tools providing insufficiently useful metadata
  - Not complete lists of dependencies (depth)
  - Incomplete or incorrect data about dependencies
- Risk: ambiguities or different interpretations in SBOM specs
  - E.g.How to take a hash
  - How to deal with “known unknowns”
- Data from different sources

Quality of Free Tools



On the Accuracy of GitHub's Dependency Graph

Daniele Bifolco
University of Sannio
Benevento, Italy

Massimiliano Di Penta
University of Sannio
Benevento, Italy

Sabato Nocera
University of Salerno
Fisciano, Italy

Rita Francese
University of Salerno
Fisciano, Italy

Simone Romano
University of Salerno
Fisciano, Italy

Giuseppe Scanniello
University of Salerno
Fisciano, Italy

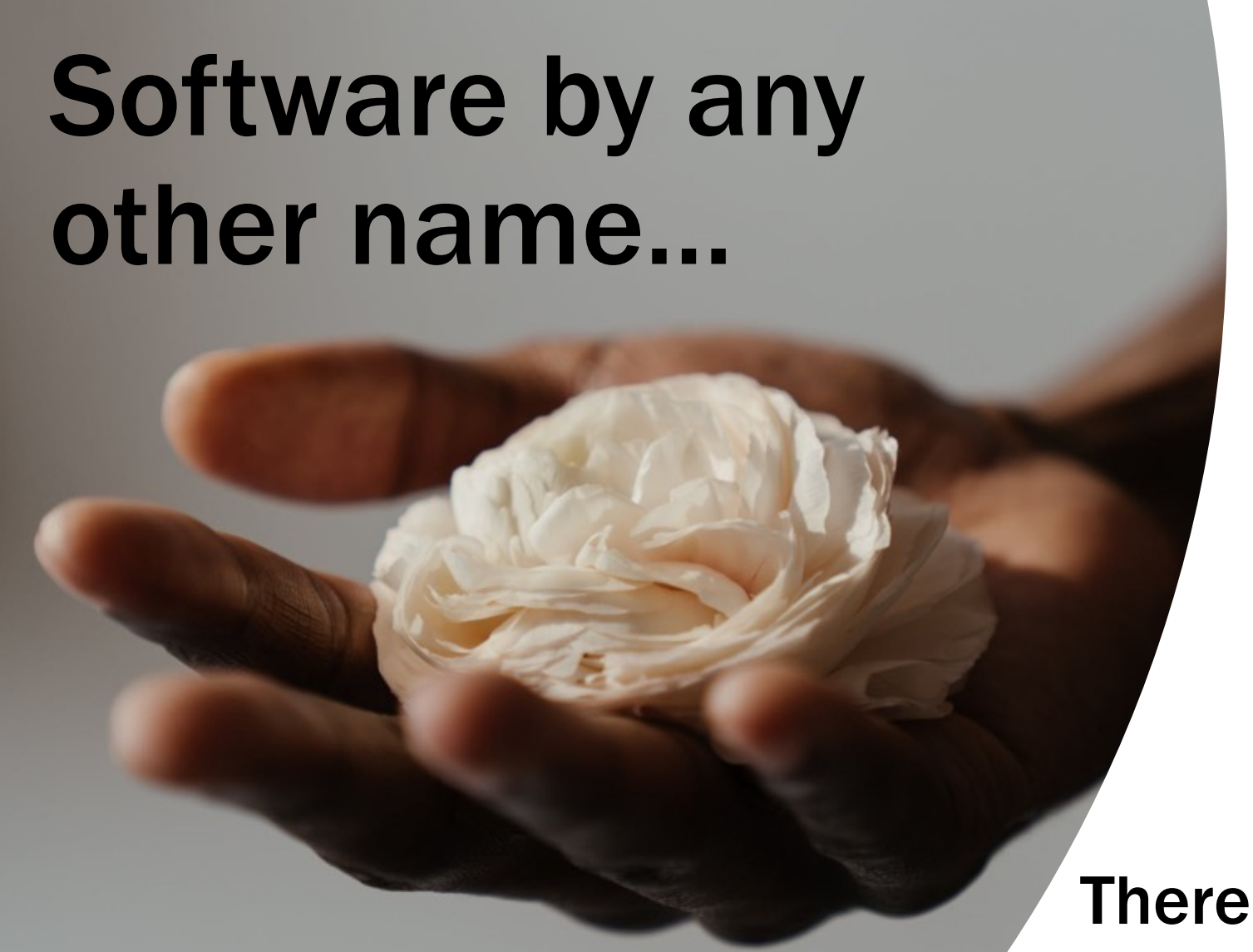
"No single tool on the market meets our needs..."

-Major US medical device manufacturer

Defining SBOM

- How do we determine whether what is generated, maintained, or shared is an SBOM?
- Defining the data fields
- Defining based on Use Cases
  - Identifying vulnerabilities
  - Mapping to other sources
- Need for global harmonization

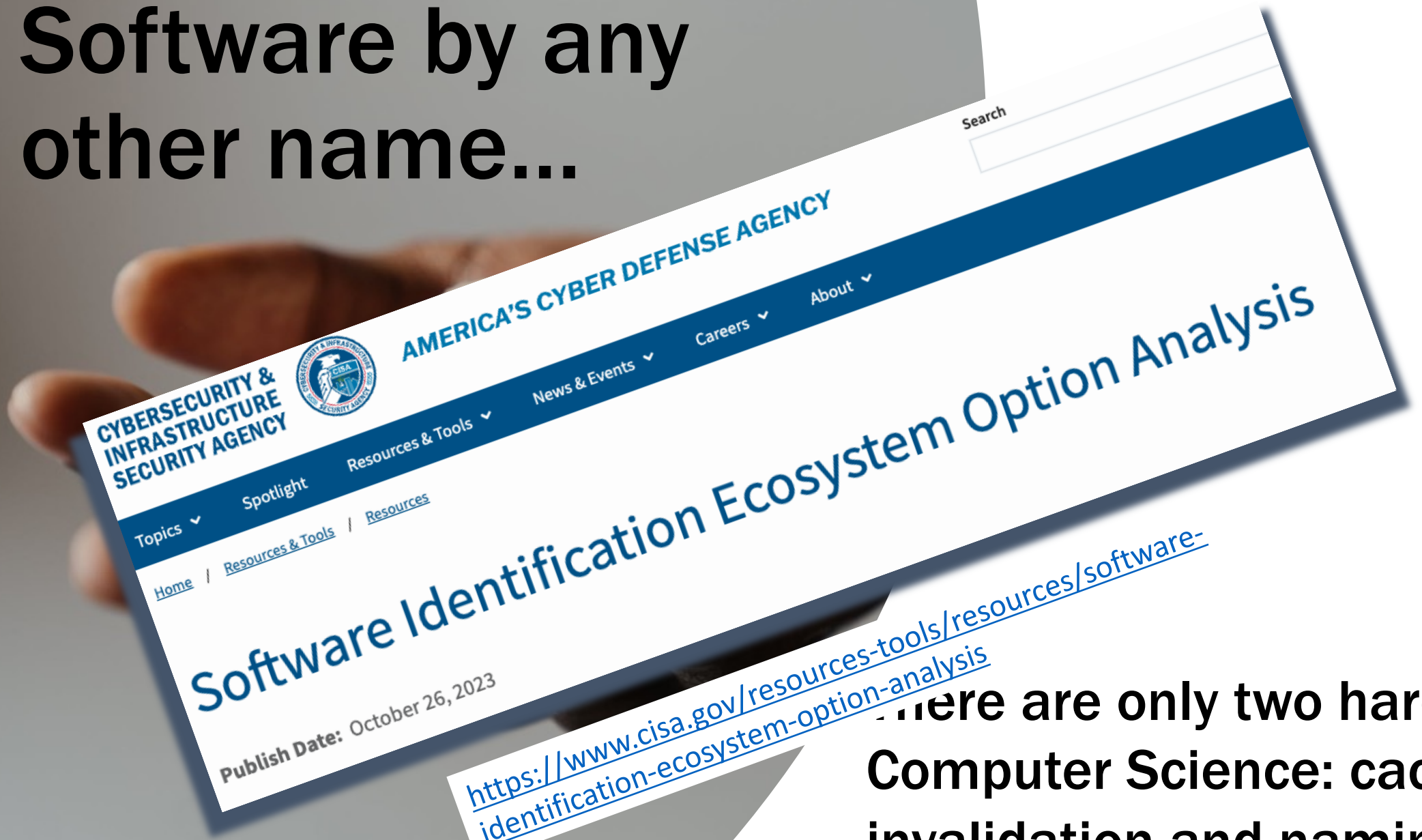
Software by any other name…



There are only two hard things in Computer Science: cache invalidation and naming things.”

- attributed to Phil Karlton

Software by any other name...



https://www.cisa.gov/resources-tools/resources/software-identification-ecosystem-option-analysis

"There are only two hard things in Computer Science: cache invalidation and naming things."

- attributed to Phil Karlton

Finding the “Known Badness”

Finding the “Known Badness”

- Research!
- Reporting
- Acknowledgement
- Assessment and Validation
- Remediation
- Disclosure

How Organizations can make CVD work

- Acknowledge the Issue
- Engage with the researchers constructively
- Provide Timely Updates
- Don’t shoot the messenger!

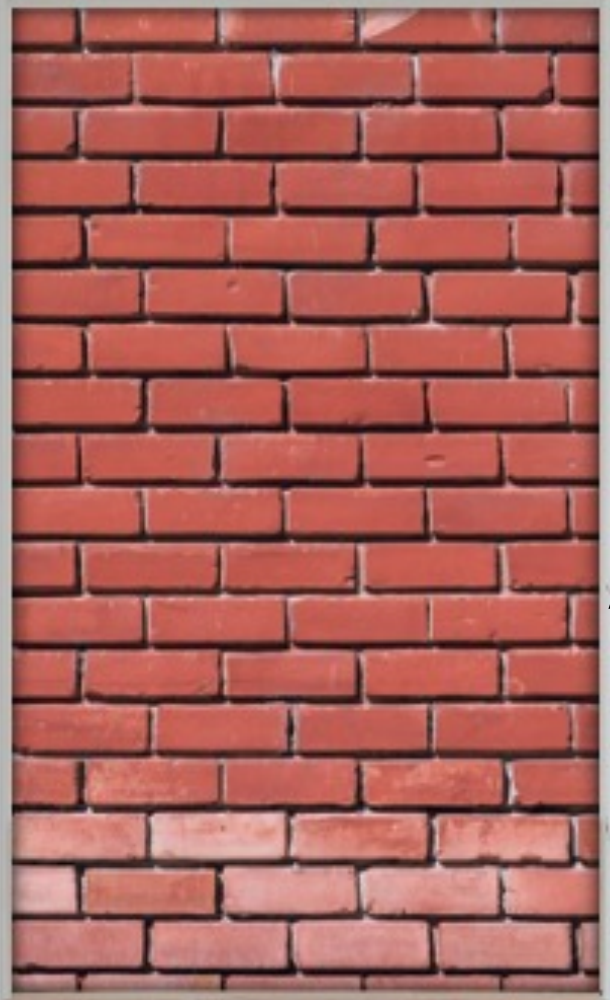

ANNOUNCEMENT
CISA Announces Vulnrichment Repository
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CISA

Not all vulnerabilities are exploitable

Not all vulnerabilities are exploitable

Vulnerability Exploitability eXchange

Not all vulnerabilities are exploitable



Component not present

Affected code not loaded

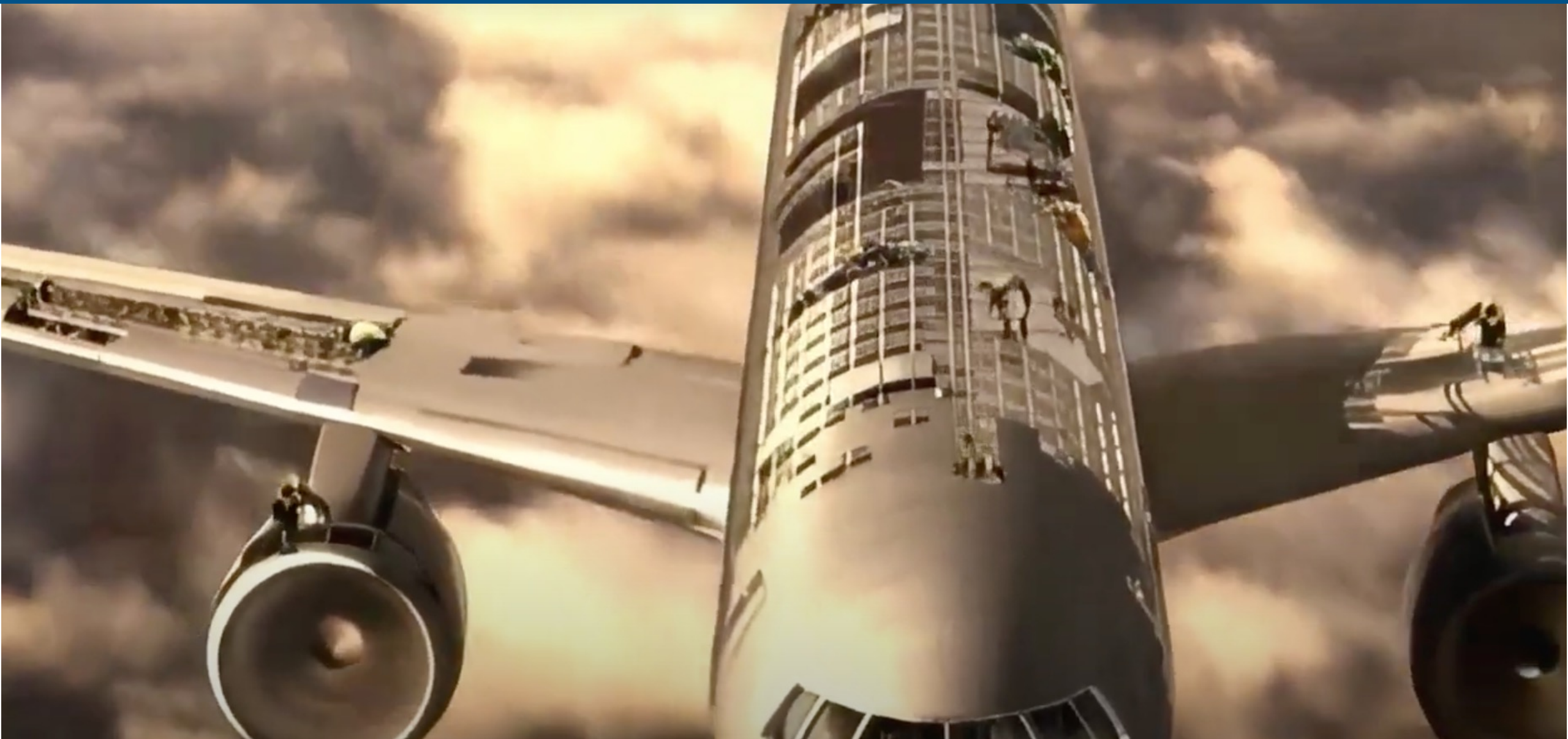
Affected code not in path

Attacker can’t touch affected code

In-line mitigations exist

What is the future going to look like?

“Building the Plane While Flying It”



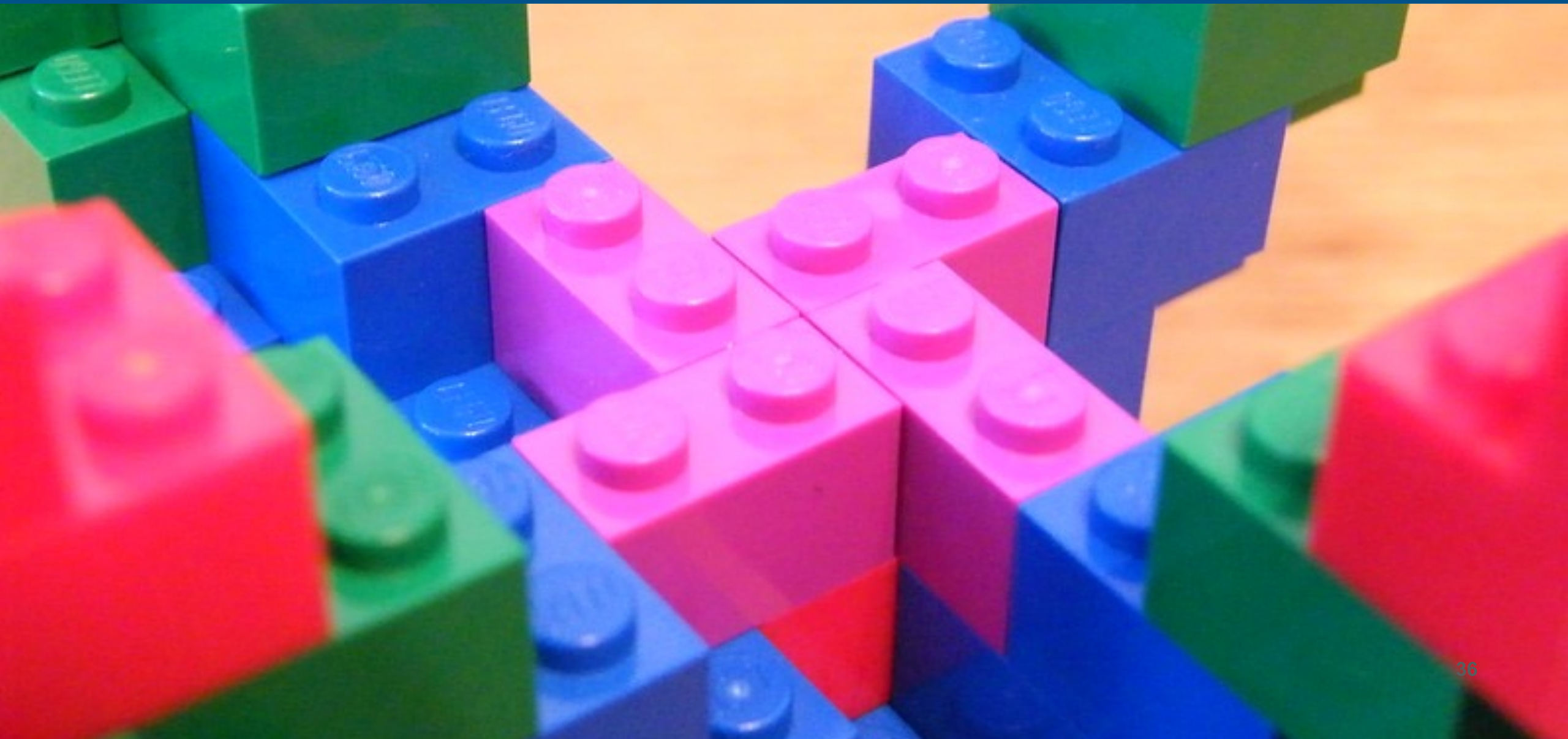
“Building the Plane While Flying It”

Better Data

Better Data for Automation

Tooling to Generate and Consume

Build Things… *With Modularity*



Build Things… *With Modularity*

Embrace an evolving world of valuable data

Get involved with any of these projects!

Email:
SBOM@cisa.dhs.gov