NDIA Working Group Project

Software Bill of Materials (SBOM)

11-02-22

NDIA System Security Engineering Working Group – SBOM Project Effort

SBOM Working Group

- Cory Ocker – Raytheon Technologies – Largo, FL
- Robert Martin – MITRE Corporation
- Bradley Landford - DoD
- Linda A Gee – Raytheon Technologies – Nashua, NH
- Joe Yuna - AFMC AFLCMC/CROWS
- Gina Hamey – DoD, AFMC AFLCMC/CROWS

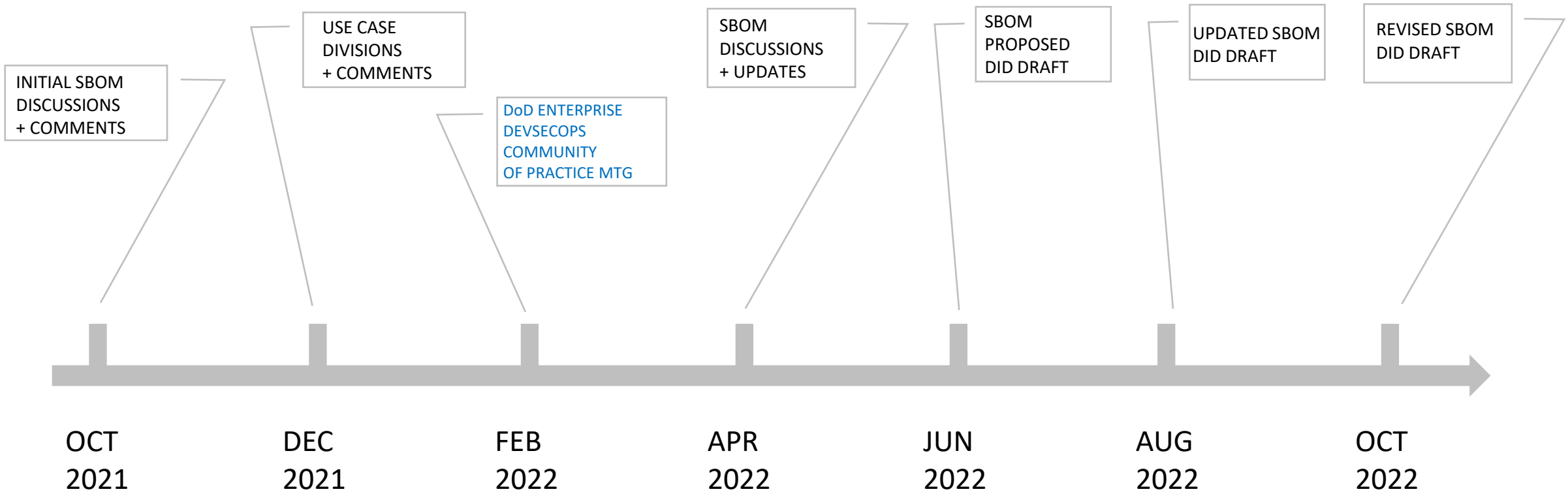
SBOM Catalyst – Executive Order 14028

Executive Order 14028 – “Improving the Nation’s Cybersecurity”

May 12, 2021

- "The trust we place in our digital infrastructure should be proportional to how trustworthy and transparent that infrastructure is...”
- The EO defines SBOM and identifies the value proposition in 10(j)
  - Section 4: Enhancing Software Supply Chain Security.4(f) –NTIA defines the “minimum elements” of SBOM
  - 4(e)(vii) –Commerce and USG defines guidance on“providing a purchaser a Software Bill of Materials (SBOM) for each product”

Timeline - Software Bill of Materials DID NDIA Project



October 2021 – Initial SBOM Discussions
12 Attributes

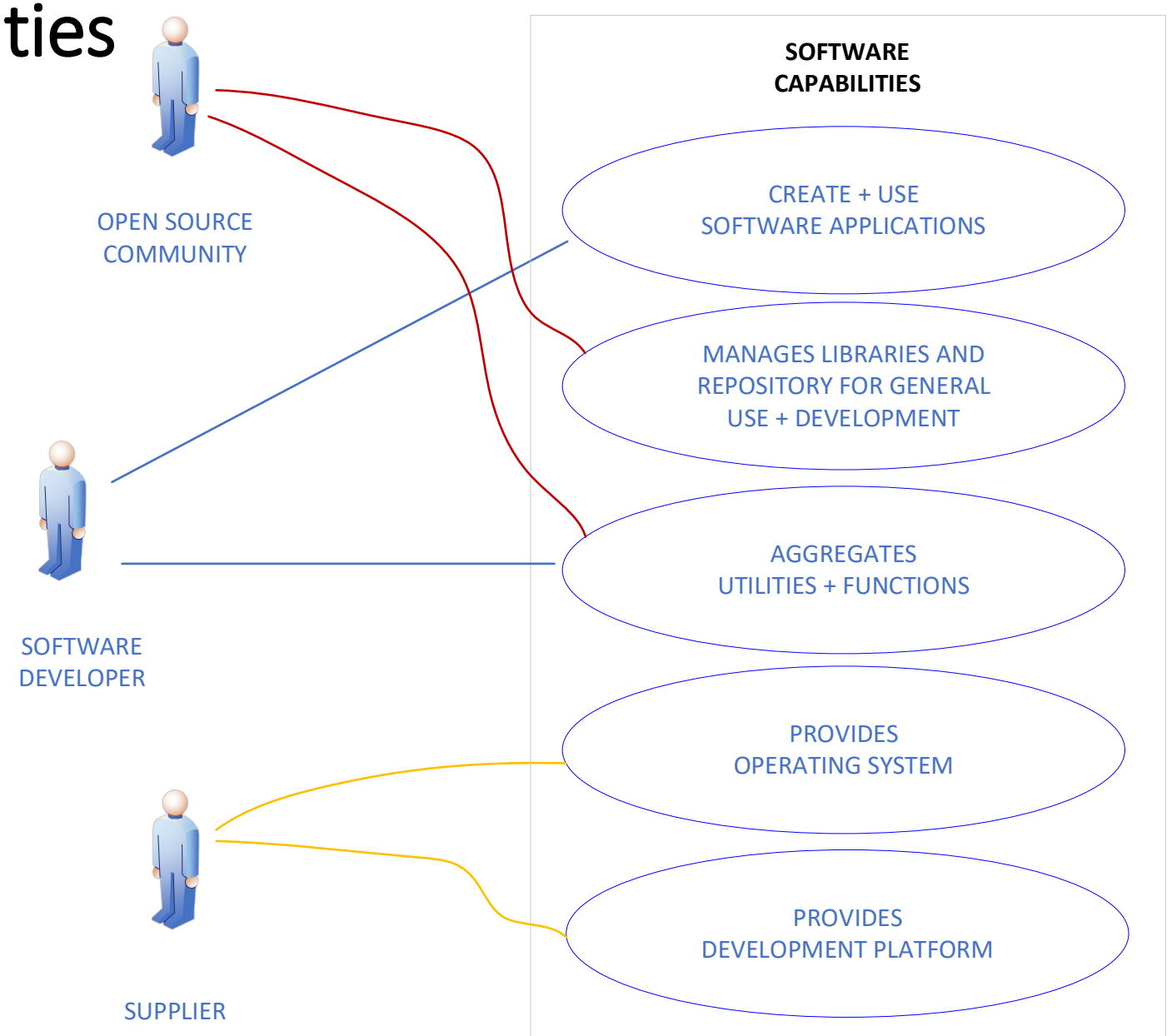
- **Supplier**
  - Provide the Supplier name
- **Description**
  - Software application name and high-level description (e.g., analysis tool, database, development infrastructure)
- **Version**
  - Software version required for effort
- **Part Number**
  - Established per effort
- **Current Version**
  - Current software version at the time of SBOM development
- **Use Requirements**
  - Support drivers for this software (can be functional or utility)
- **Dependencies**
  - Software dependencies for platform, OS, other applications, etc
- **Maintenance / Updates / Tuning Frequency**
  - Recommended maintenance, updates and tuning
- **Key planned releases / Updates / Sunset**
  - Published (at the time of SBOM development)
- **Patches**
  - Current patches (at the time of SBOM development)
- **Security Notes**
  - Any known CVEs
- **Supplier Contact Info**
  - Point of contact, Address, Phone

December 2021 – Use Case Perspective

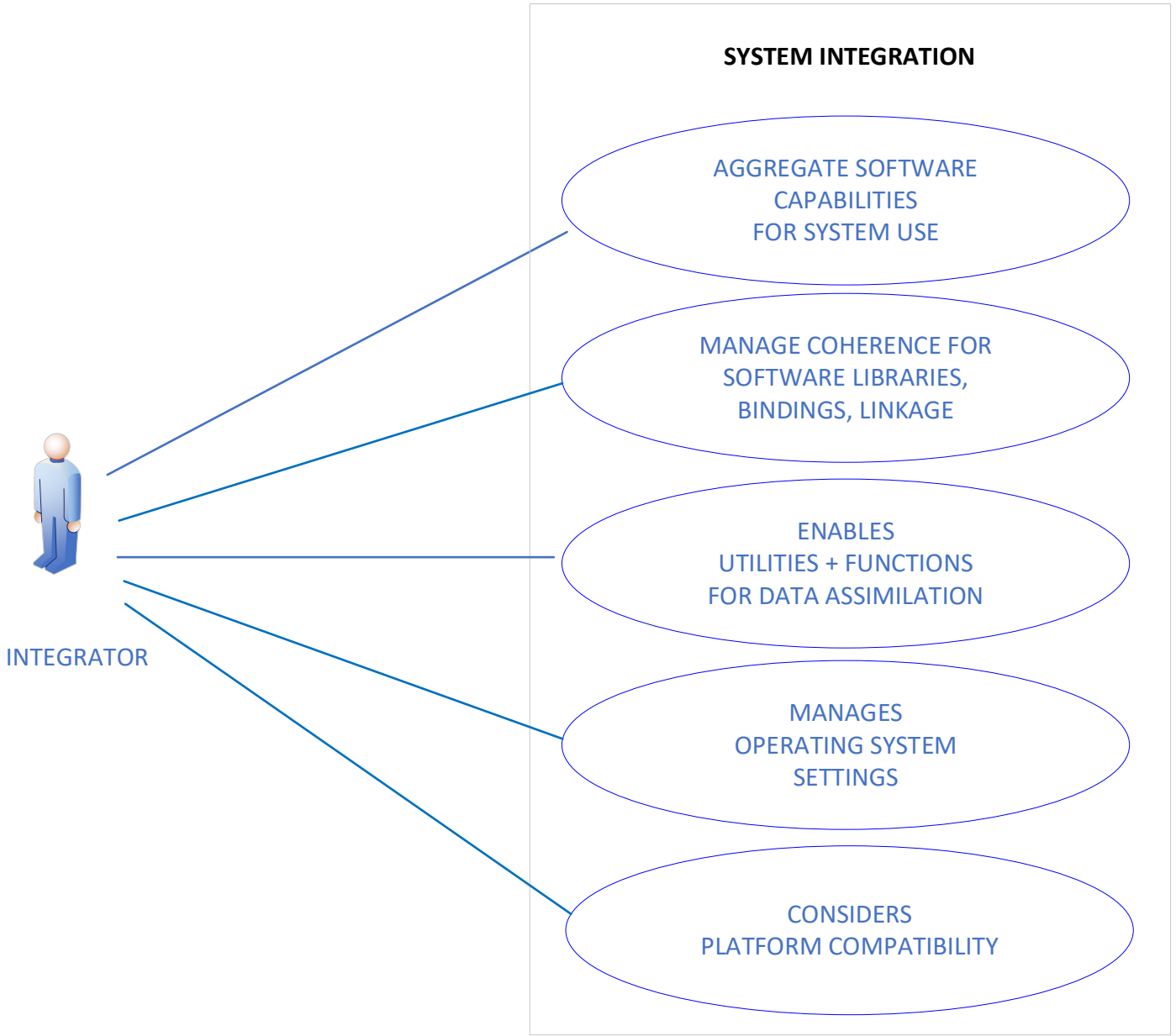
There are (3) Use Cases to define the following actors related to development and the corresponding SBOM

- **Developer: Bottoms up approach**
  - Software versions/updates, tool dependencies, development platform considerations
  - Awareness of known vulnerabilities and security risks at time of development
  - Planned delta updates/revisions
- **Integrator: Top-down approach**
  - Awareness of any known issues software/hardware/firmware compatibilities
  - Alternate components
  - Planned obsolescence, near-term obsolescence
- **Tester: System approach**
  - Application versions, application data outputs and formats, interfaces, triggers, required initial conditions
  - Critical operation thread and components
  - Developmental test perspective only

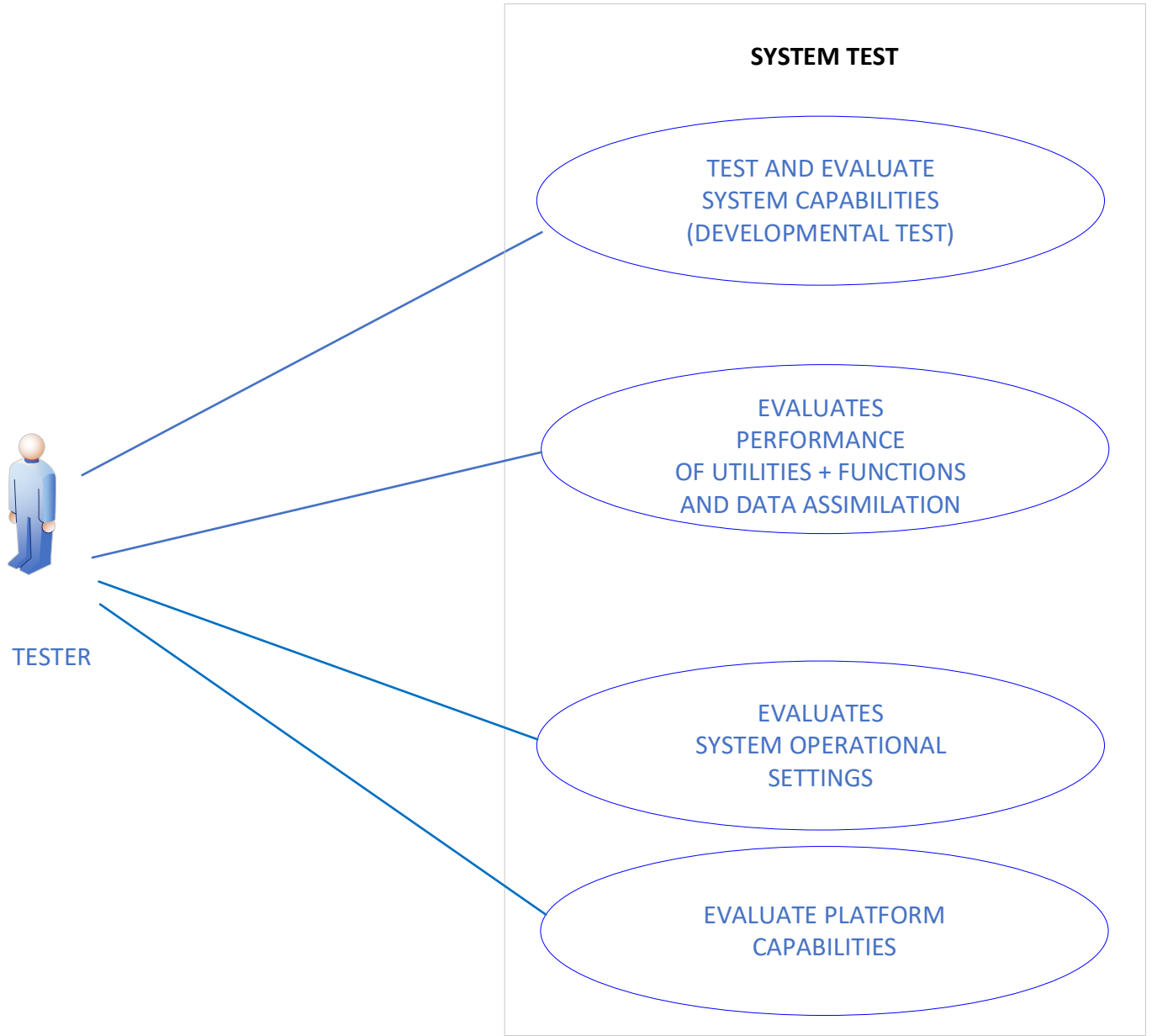
Use Case – Basic Definition: Developer Software Capabilities



Use Case – Basic Definition: Integrator



Use Case – Basic Definition: Tester



Friedman's 2022 Perspective *

*Material reference:
CISA - Dr Allan Friedman
Presentation: SBOM Progress Made, Work to be Done
2-10-22

The State of SBOM in 2022

- Tooling is still emerging, especially for consumption.
- Assumptions about seamless interoperability have not been tested.
- No proven scalable tools for sharing & exchanging SBOM data.
- Not all vulnerabilities put organizations at risk.

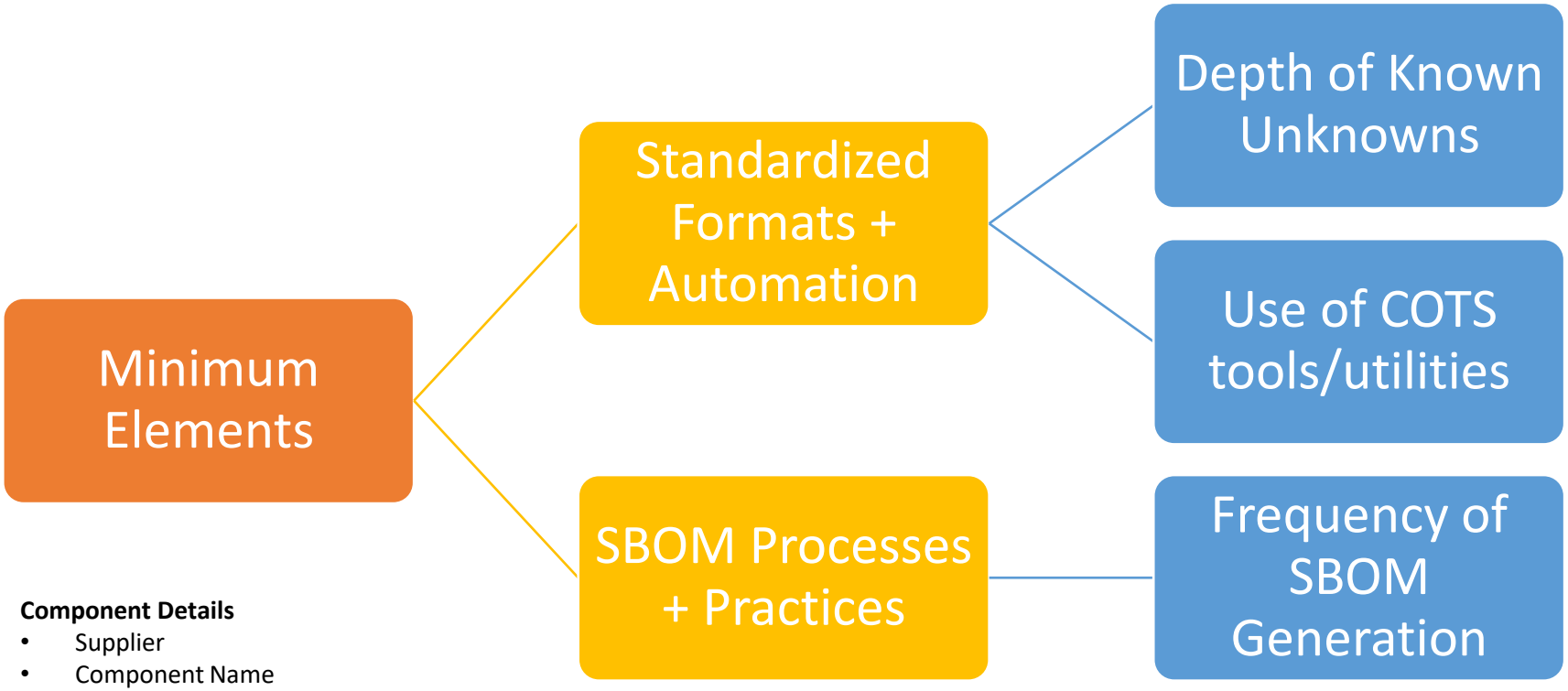
There is no reason organizations cannot use SBOM today, but we cannot assume universal full automation and integration.

Allan Friedman
February 14, 2022

33

SBOM Takeaways from Dr Allan Friedman *

*Material reference:
CISA - Dr Allan Friedman
Presentation: SBOM Progress Made, Work to be Done
2-10-22



Component Details
- Supplier
- Component Name
- Version of Component
- Unique identifiers
- Dependency relationship
- SBOM Author
- Timestamp

Beyond Minimum Elements
- Hash, lifecycle phase, license info
- Cloud-based SW, Software as a Service
- SBOM integrity + authenticity
- Vulnerabilities + SBOM
- Exploitability + vulnerabilities in SBOM
- Legacy SW + binary analysis
- Flexibility vs uniformity in implementation

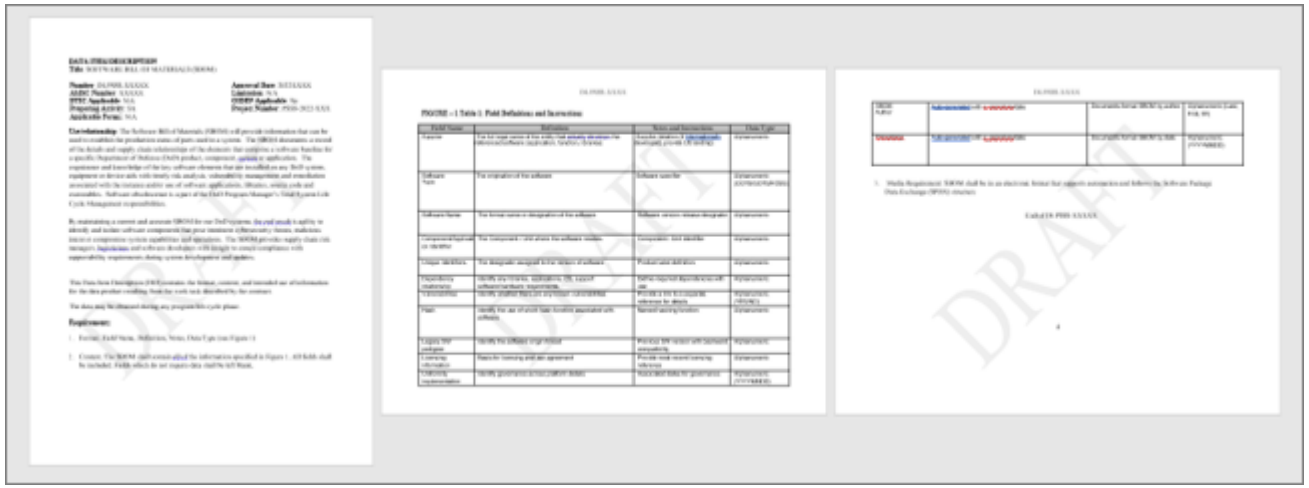
Broader SBOM Use Cases

April 2022 - Considerations and Next Steps

- Define the context and operating parameters for the three use cases defined
  - Integrator Use Case is the most impactful for development extensions
- Focus on identifying what is necessary for the SBOM versus what is considered metadata
- Consider the phases: Development – Deployment – Operations

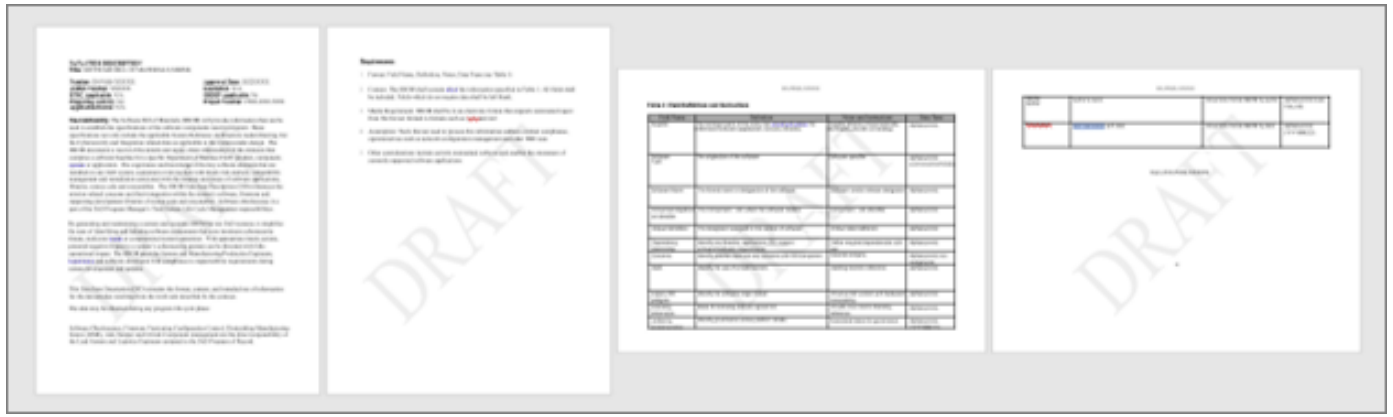
Initial Draft SBOM DID – June 2022

- Common baseline components
  - “Common denominators”
- Represents a snapshot in time
- Sensitive detail considerations
  - Metadata



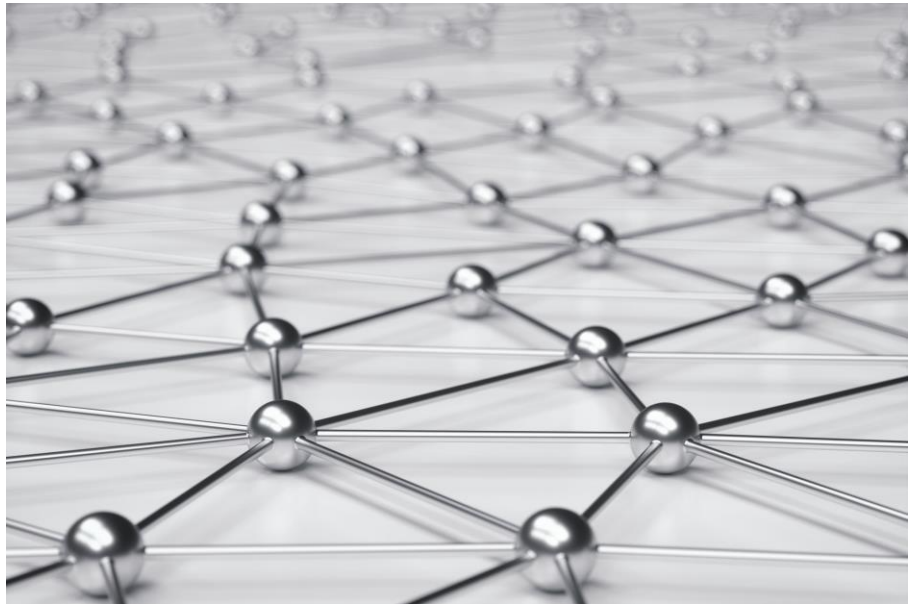
Updated Draft SBOM DID - Internal Comments
SBOM Working Group

- Updated and expanded explanatory text
- DID element context
- Generalized format for automated readers



Revised Draft SBOM DID
Comments from SSE Working Group

- Received 130+ comments from
  - Boeing
  - Lockheed Martin
  - AFLCMC/EZS
  - Booz Allen
  - Software Engineering Institute
  - Raytheon
  - Northrup Grumman



- Comments
  - Use / relationship
  - DID Requirements

Challenges and Continued Discussion
SBOM Considerations

- SBOM delivery and format
- Security classification and handling
- Explicit data formats
- Software identification tags
- Software types
- Unique identifiers
- Governance
- SBOM generation - points of contact

Path Forward
Actions and Next Revision SBOM DID

- Continue SBOM DID discussions with the SSE Working Group
- Release for review and collect comments from other NDIA functional working groups beyond SSE
- Stay current with other SBOM efforts within the DoD community
- Final document to be sent to Ms Melinda Reed OUSD(R&E) to coordinate internally with the USG before being added to the Assist Database