309 SWEG Supply Chain Risk Management Software Support Center

USAF Software: SBOM/C-SCRM Efforts

Parker Bauer
USAF/AFMC/AFSC/309 SWEG
Alexander Wright
USAF/AFMC/AFSC/309 SWEG

Overview

- Background
- On-Site Technical Supplier C-SCRM Assessments
- USAF Software SBOM R&D Efforts
- DoD/NNSA Software Assurance CoP SBOM WG Update
- Discussion

Background

Who We Are

- ## Parker Bauer
  - Computer Scientist/Mechanical Engineer
  - Six Sigma Black Belt
  - Director of USAF Software Technology Support Center
  - Private industry supplier quality auditor
  - Hill AFB
  - Co-lead of USAF 309 SWEG SCRM SSC since 2019

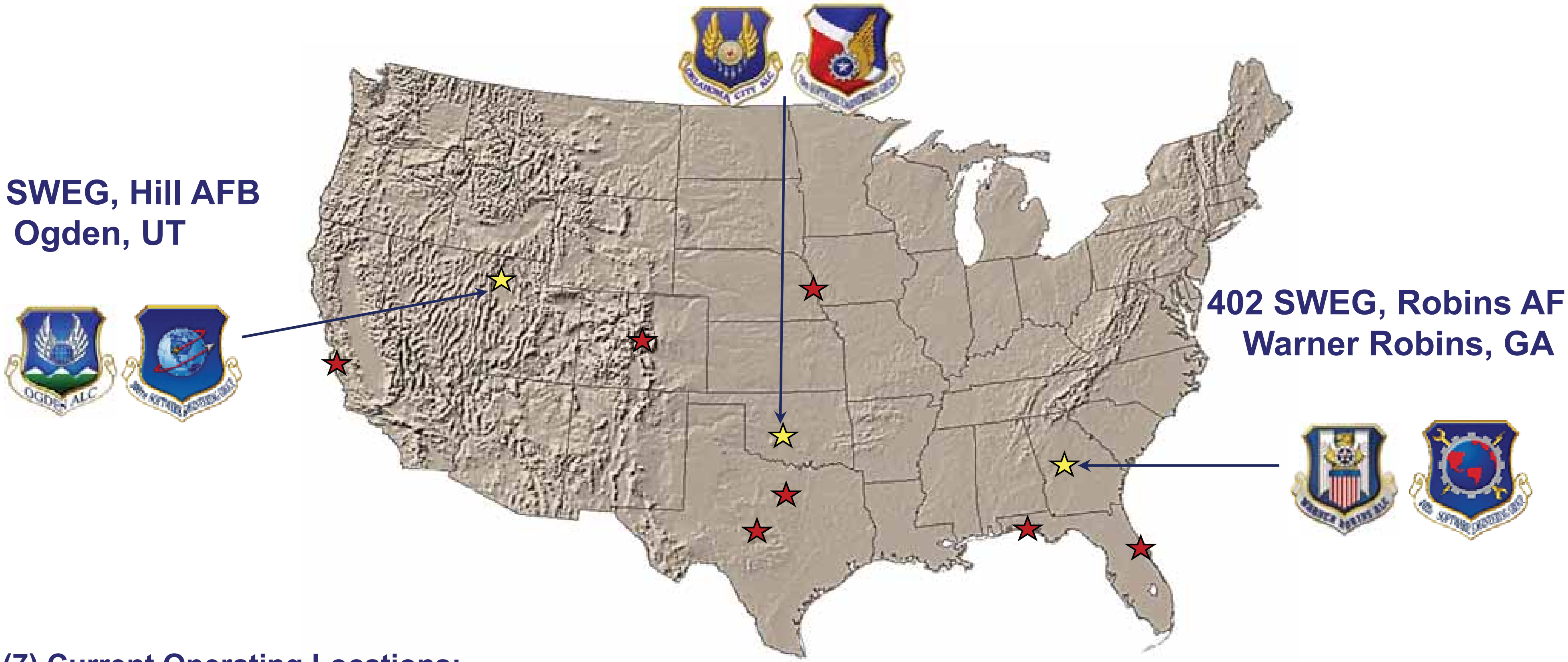
- ## Alexander Wright
  - Computer scientist and a member of the 309 Software Engineering Group.
  - Have worked on numerous air and space systems and became involved in SCRM in 2018
  - Peterson SFB
  - Co-lead of USAF 309 SWEG SCRM SSC since 2019

Background
USAF AFSC Software Directorate

76 SWEG, Tinker AFB
Oklahoma City, OK

309 SWEG, Hill AFB
Ogden, UT

402 SWEG, Robins AFB
Warner Robins, GA



★ **Seven (7) Current Operating Locations:**
Vandenberg AFB, CA – Peterson SFB, CO – NAS JRB, TX – JBSA, TX – Offutt AFB, NE – NAS Pensacola, FL – Patrick SFB, FL

Background
USAF AFSC Software Directorate

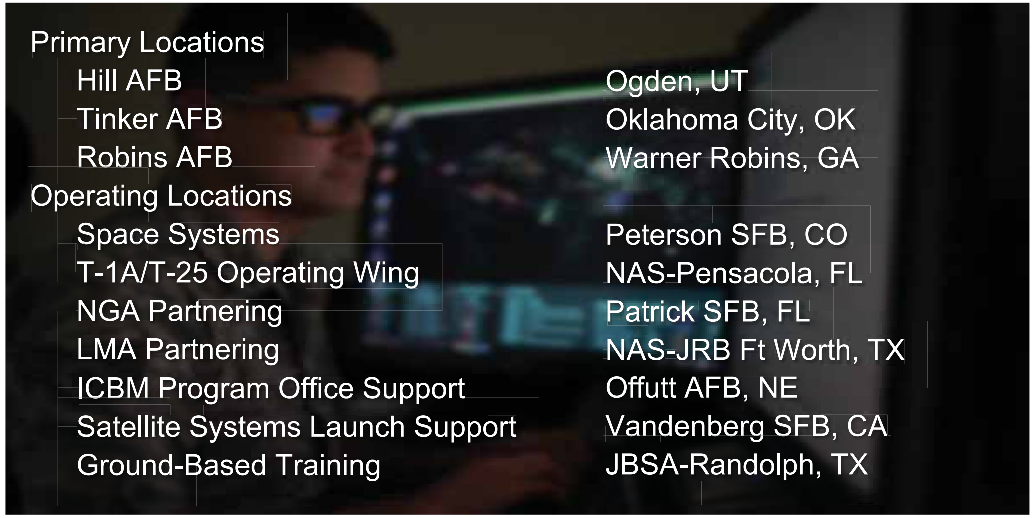
Organizational Facts

- 3 Air Force Groups united under **AFSC/SW**
- Supporting the warfighter since **1978**
- **5,000+** software professionals
- **3** primary and **7** Operating Locations (OLs)
- Proven ability to expand **8% annually**
- FY23 annual revenue **$1.04B**
- **11** AFLCMC supported PEOs
- **100+** active projects
- Robust **community**, **academic**, and **industry partnerships**

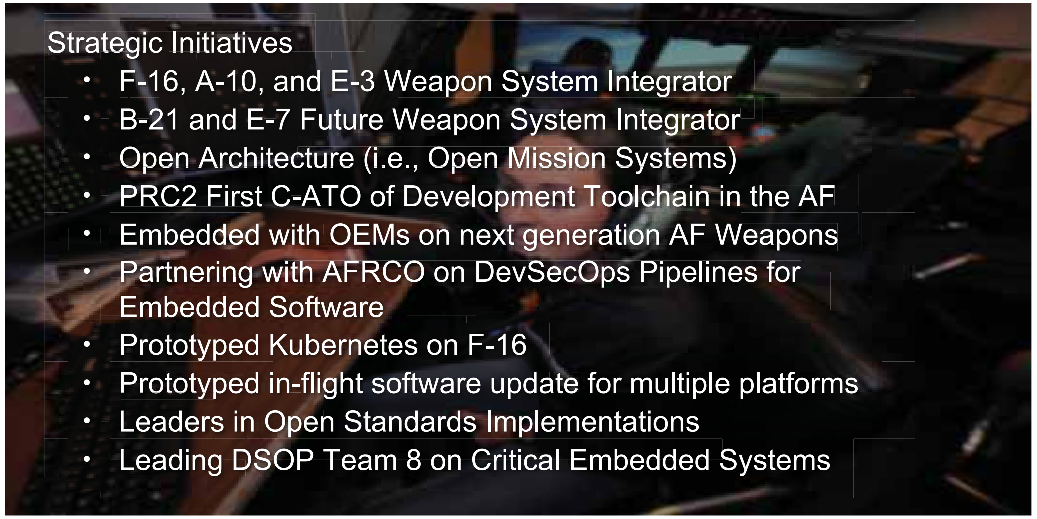
Develop, deliver, support, and sustain war-winning capabilities

Mission and Product Lines

- Embedded Weapon System Systems and Software Development
- Primary Product Lines:
  - Platform Integration
  - Mission Computing
  - Weapons
  - Air Vehicle Systems
  - Sensor Systems
  - Mission Support
  - Pilot Vehicle Interface
  - Business Systems



Primary Locations	
Hill AFB	Ogden, UT
Tinker AFB	Oklahoma City, OK
Robins AFB	Warner Robins, GA
Operating Locations	
Space Systems	Peterson SFB, CO
T-1A/T-25 Operating Wing	NAS-Pensacola, FL
NGA Partnering	Patrick SFB, FL
LMA Partnering	NAS-JRB Ft Worth, TX
ICBM Program Office Support	Offutt AFB, NE
Satellite Systems Launch Support	Vandenberg SFB, CA
Ground-Based Training	JBSA-Randolph, TX



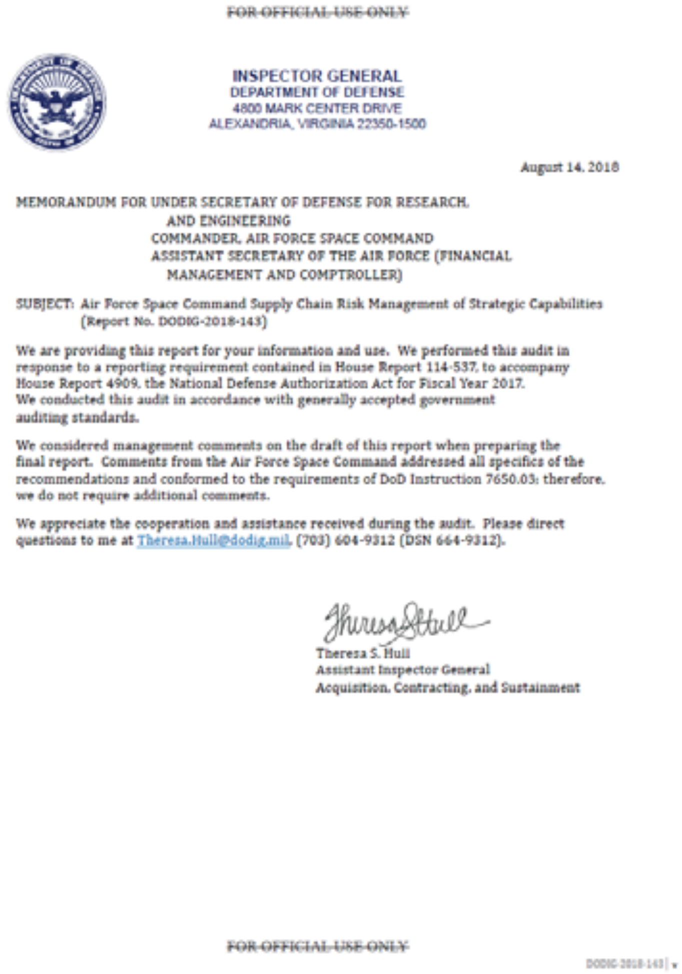
Strategic Initiatives

- F-16, A-10, and E-3 Weapon System Integrator
- B-21 and E-7 Future Weapon System Integrator
- Open Architecture (i.e., Open Mission Systems)
- PRC2 First C-ATO of Development Toolchain in the AF
- Embedded with OEMs on next generation AF Weapons
- Partnering with AFRCO on DevSecOps Pipelines for Embedded Software
- Prototyped Kubernetes on F-16
- Prototyped in-flight software update for multiple platforms
- Leaders in Open Standards Implementations
- Leading DSOP Team 8 on Critical Embedded Systems

On-Site Technical
Supplier C-SCRM Assessments

Background
AFSPC C-SCRM Effort

- **DODIG-2018-143**
  - **‘It’s not enough to trust what suppliers tell us. The DoD must validate what they tell us.’ (Trust but verify.)**



~~FOR OFFICIAL USE ONLY~~

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500

August 14, 2018

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE FOR RESEARCH,
AND ENGINEERING
COMMANDER, AIR FORCE SPACE COMMAND
ASSISTANT SECRETARY OF THE AIR FORCE (FINANCIAL
MANAGEMENT AND COMPTROLLER)

SUBJECT: Air Force Space Command Supply Chain Risk Management of Strategic Capabilities (Report No. DODIG-2018-143)

We are providing this report for your information and use. We performed this audit in response to a reporting requirement contained in House Report 114-537, to accompany House Report 4909, the National Defense Authorization Act for Fiscal Year 2017. We conducted this audit in accordance with generally accepted government auditing standards.

We considered management comments on the draft of this report when preparing the final report. Comments from the Air Force Space Command addressed all specifics of the recommendations and conformed to the requirements of DoD Instruction 7650.03; therefore, we do not require additional comments.

We appreciate the cooperation and assistance received during the audit. Please direct questions to me at Theresa.Hull@dodig.mil, (703) 604-9312 (DSN 664-9312).

Theresa S Hull

Theresa S. Hull
Assistant Inspector General
Acquisition, Contracting, and Sustainment

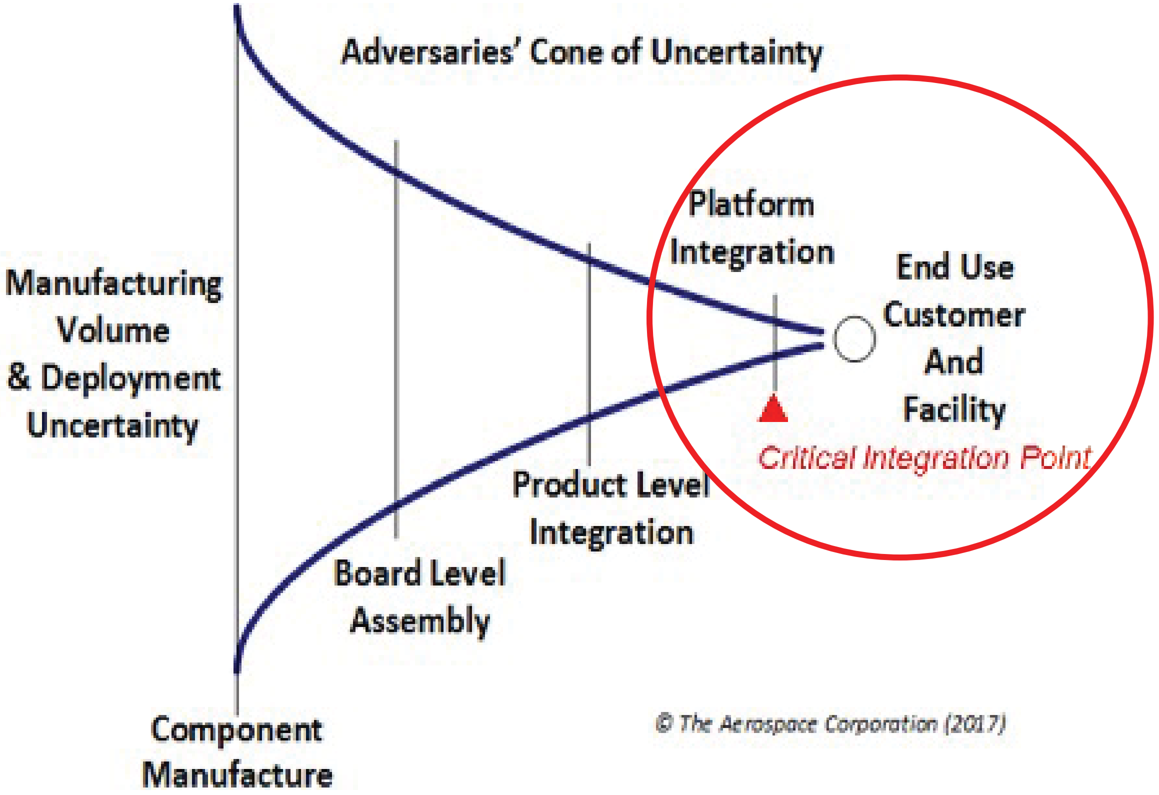
~~FOR OFFICIAL USE ONLY~~

DODIG-2018-143 | v

Background
AFSPC C-SCRM Effort

- Enterprise Ground Services (EGS) Program
  - Validate C-SCRM posture of 4 major OEM IT hardware suppliers
    - Cisco, HPe, Dell and Oracle
    - To address IG concerns
    - Via On-site Technical C-SCRM Assessments
  - Assigned Aerospace Corp to develop C-SCRM assessment framework (based on NIST 800-161 (RMF))
  - Engaged USAF 309 Software Engineering Group's software expertise

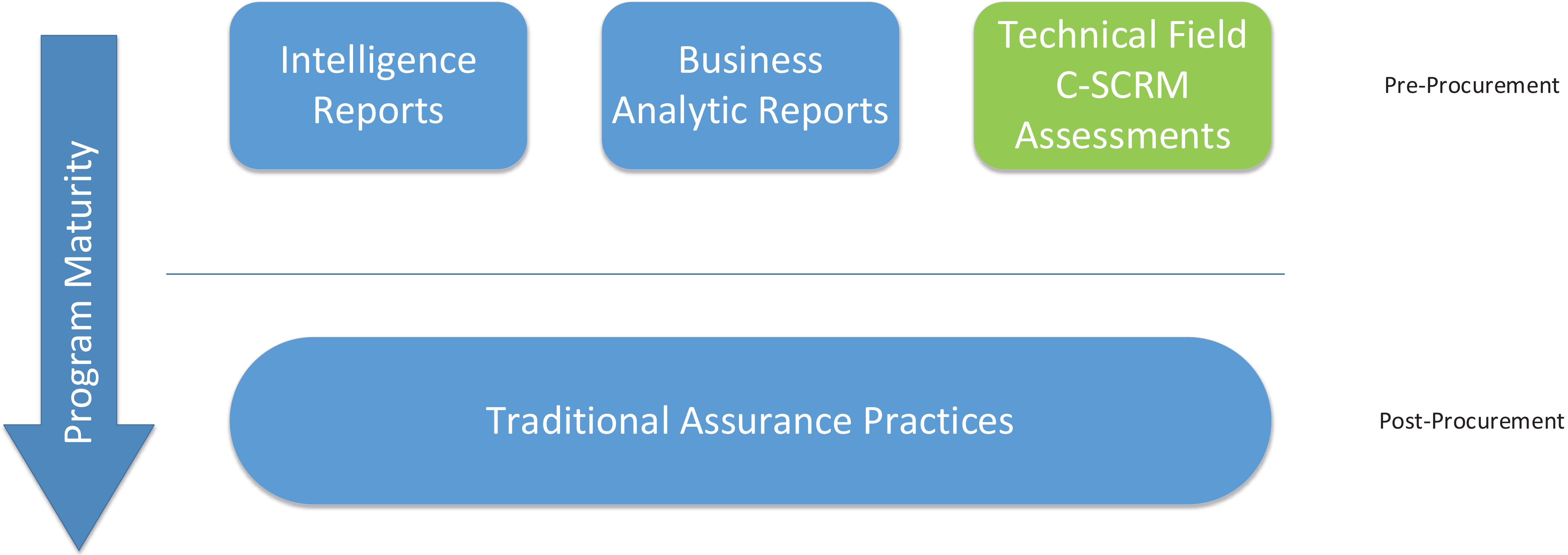
On-Site Technical Supplier C-SCRM Assessments
Which Suppliers?



Adversaries' Cone of Uncertainty
Manufacturing Volume & Deployment Uncertainty
Platform Integration
End Use Customer And Facility
Critical Integration Point
Product Level Integration
Board Level Assembly
Component Manufacture

© The Aerospace Corporation (2017)

On-Site Technical Supplier C-SCRM Assessments When?



Program Maturity

Intelligence Reports

Business Analytic Reports

Technical Field C-SCRM Assessments

Pre-Procurement

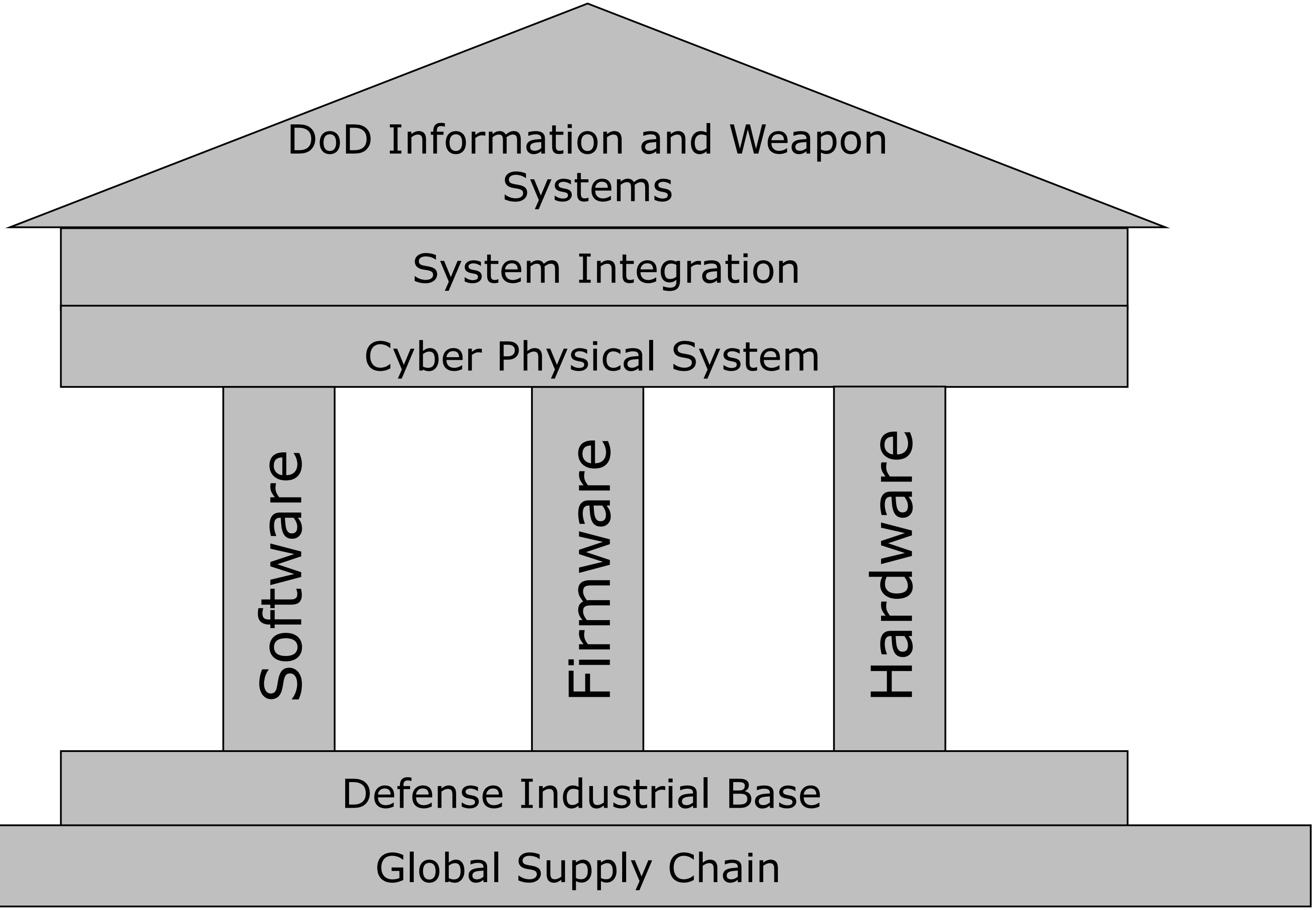
Traditional Assurance Practices

Post-Procurement

On-Site Technical Supplier C-SCRM Assessments Why?

- IG report – “validate”
- Limited view when not intrusive
  - Discovered a 3rd party manufacturing significant internet hardware for a top-tier industry supplier that was not discoverable on a commercial supply chain search
  - Observed dedicated DoD or USG development and integration facilities to understand cyber posture
  - Also allows for follow-up for improvements in SCRM posture
- Private sector companies perform intrusive audits for multiple purposes – financial, quality (ISO/AS), etc. Best practice to not rely exclusively on desk audits.

On-Site Technical Supplier C-SCRM Assessments What is Assessed?



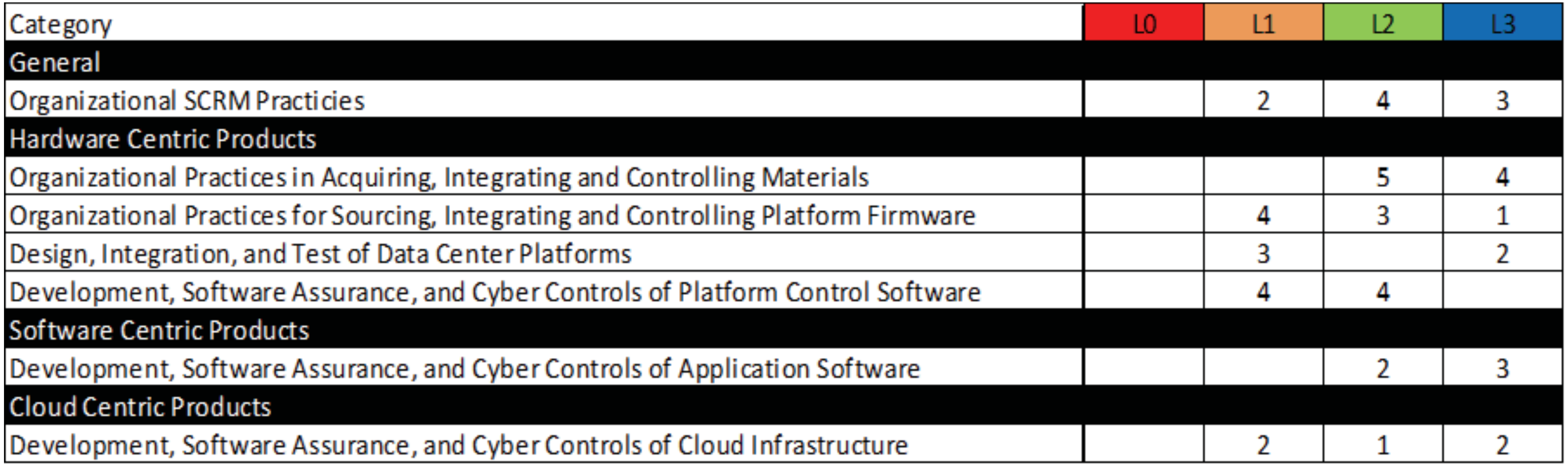
On-Site Technical Supplier C-SCRM Assessments
What is Assessed?

Assessment Categories

- General Organizational SCRM Practices
- Hardware Centric Products
  - Design & Test
  - Integration
  - Platform Firmware
  - Platform Software
- Software Centric Products
- Cloud Centric Products

On-Site Technical Supplier C-SCRM Assessments
What are the results?

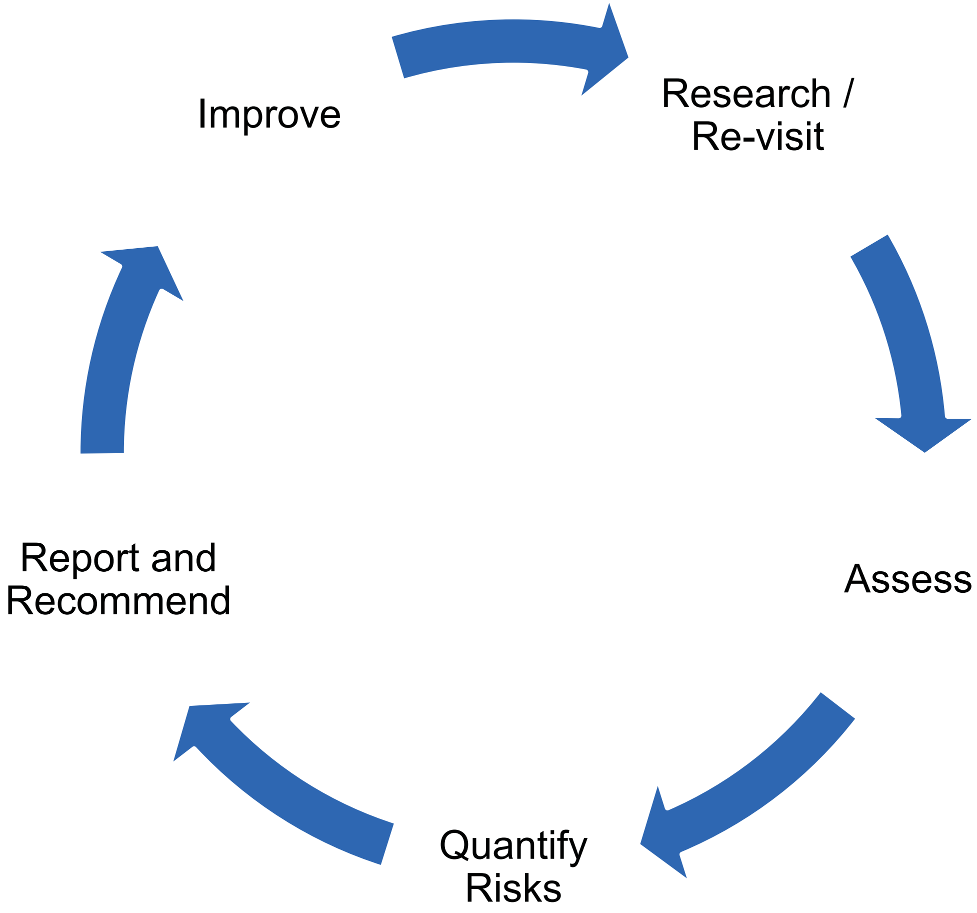
Summary of number of observations at each risk level in each category.



Category	L0	L1	L2	L3
General				
Organizational SCRM Practices		2	4	3
Hardware Centric Products				
Organizational Practices in Acquiring, Integrating and Controlling Materials			5	4
Organizational Practices for Sourcing, Integrating and Controlling Platform Firmware		4	3	1
Design, Integration, and Test of Data Center Platforms		3		2
Development, Software Assurance, and Cyber Controls of Platform Control Software		4	4	
Software Centric Products				
Development, Software Assurance, and Cyber Controls of Application Software			2	3
Cloud Centric Products				
Development, Software Assurance, and Cyber Controls of Cloud Infrastructure		2	1	2

- **Example of a risk identified for PPP: If Supplier X signing servers are not separated from the development network, then there is the risk of insider threats being able to pass a malware payload as legitimate to software products.**
- **Additional risks are also documented.**

On-Site Technical Supplier C-SCRM Assessments
What happens after the initial assessment?



Improve

Research / Re-visit

Assess

Quantify Risks

Report and Recommend

On-Site Technical Supplier C-SCRM Assessments Summary

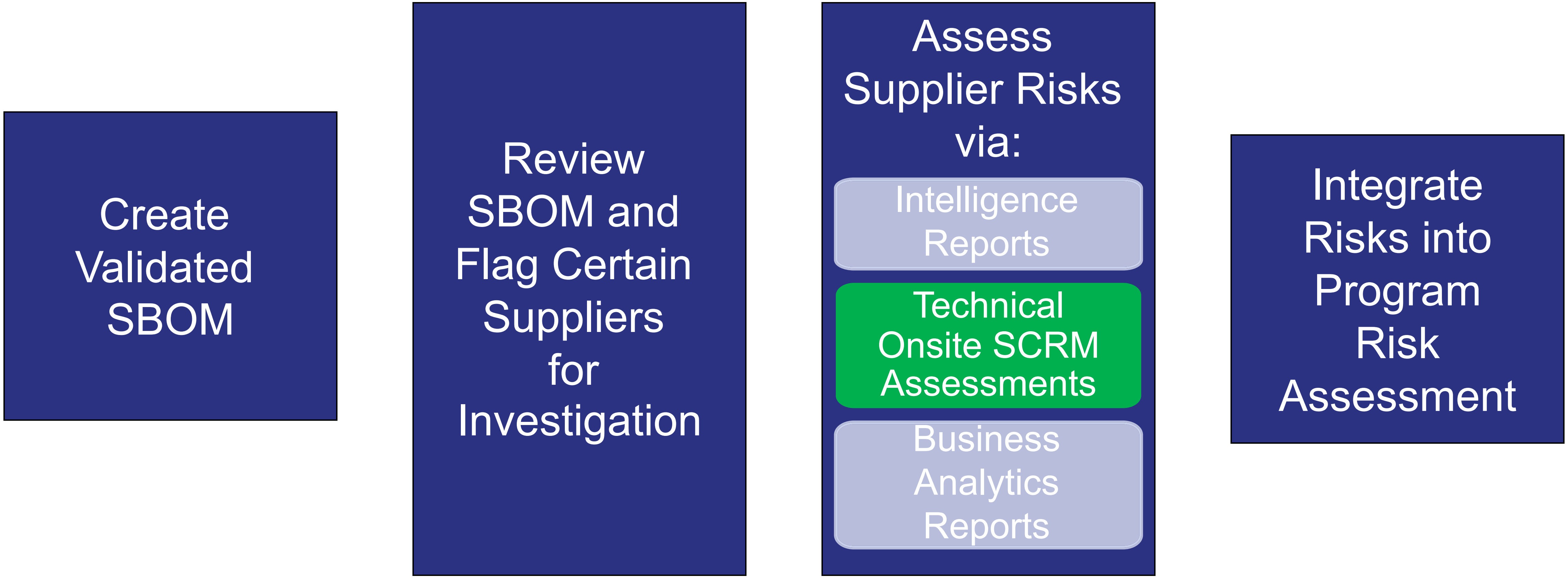
- Another tool for DoD programs to assess and reduce supplier risks
- Suppliers assessed to date have welcomed the results as it has helped them improve their risk posture
- Best performed prior to acquisition of a major weapon system but applicable at any point in the acquisition lifecycle

USAF Software SBOM R&D Efforts

USAF Software SBOM R&D Efforts
Why?

- **Initiated our Software SBOM effort…**
  - **Because we realized it is the foundation for our Software SCRM effort**
  - **Since we will likely need to create SBOMs for our organically developed software once policy matures and we wanted to …**
    - **provide input to policy that we will eventually need to follow**
    - **establish our own work processes around SBOM before required to**
    - **investigate tools for the various activities around SBOMs**

USAF Software SBOM R&D Efforts
Why SBOM is Important



Create Validated SBOM

Review SBOM and Flag Certain Suppliers for Investigation

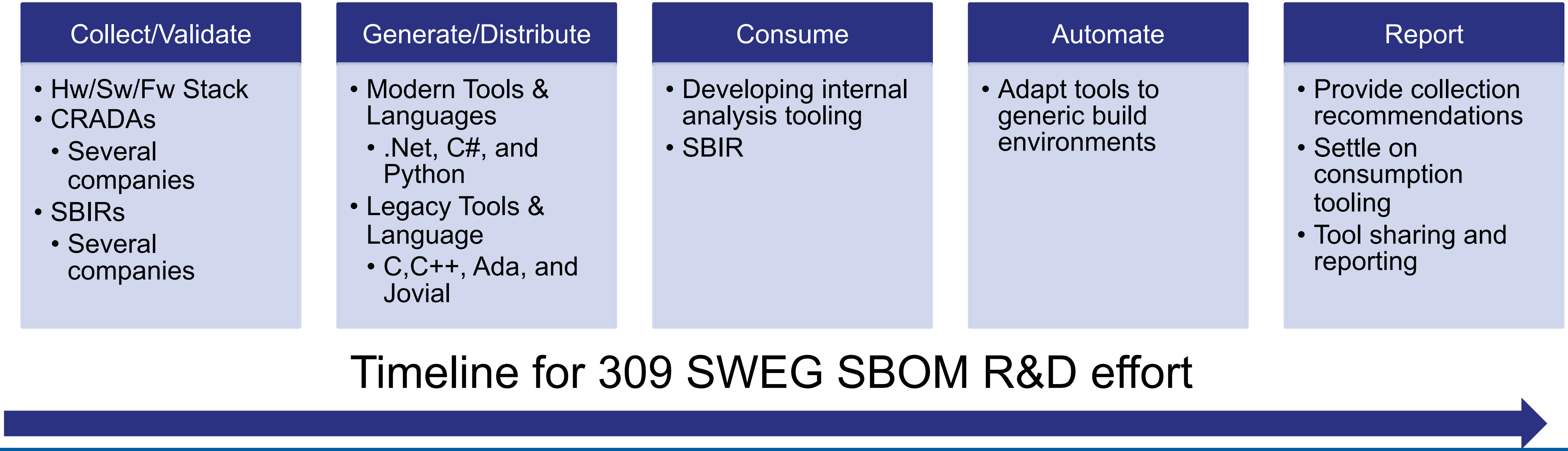
Assess Supplier Risks via:

- Intelligence Reports
- Technical Onsite SCRM Assessments
- Business Analytics Reports

Integrate Risks into Program Risk Assessment

USAF Software SBOM R&D Efforts
Effort Summary

- The 309 SWEG is actively generating SBOMs, and its members are integrating with the 309th SWEG SCRM IPT:
  - SBOM integration using modern technologies
  - SBOM generation for legacy technologies and systems
  - SBOM collection from upstream suppliers
  - SBOM consumption to find vulnerabilities and adversarial exploits



Collect/Validate
- Hw/Sw/Fw Stack
- CRADAs
  - Several companies
- SBIRs
  - Several companies

Generate/Distribute
- Modern Tools & Languages
  - .Net, C#, and Python
- Legacy Tools & Language
  - C,C++, Ada, and Jovial

Consume
- Developing internal analysis tooling
- SBIR

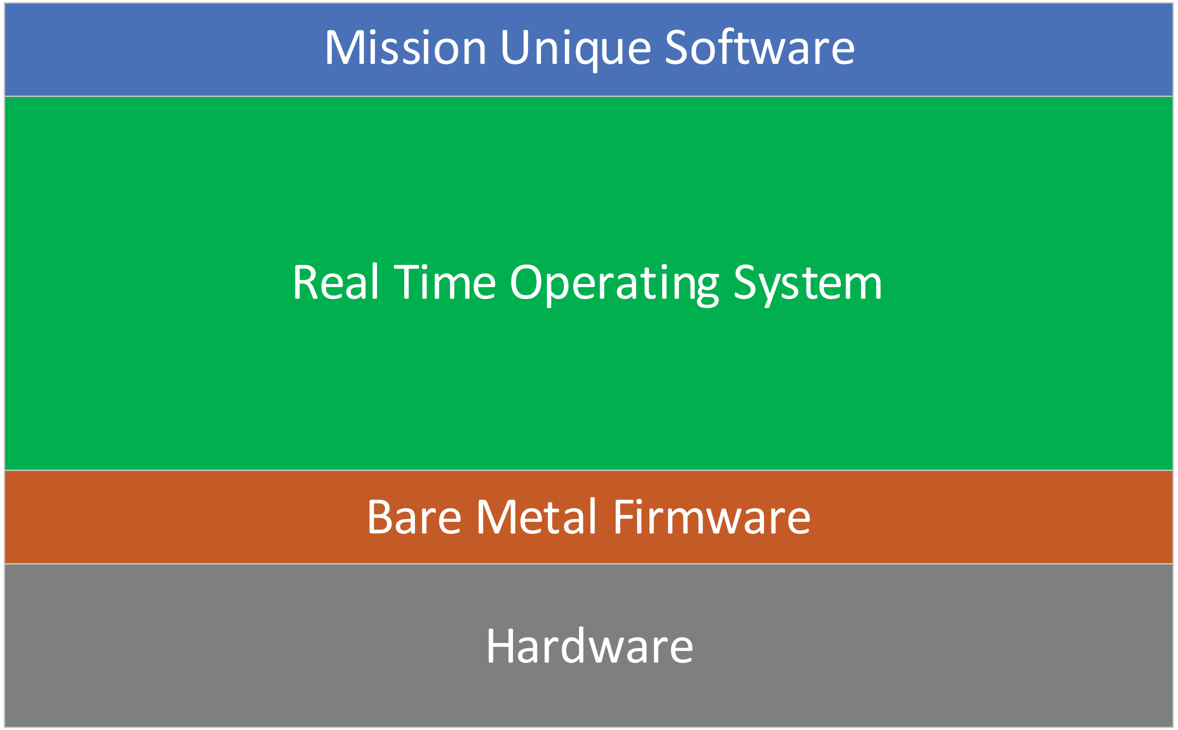
Automate
- Adapt tools to generic build environments

Report
- Provide collection recommendations
- Settle on consumption tooling
- Tool sharing and reporting

Timeline for 309 SWEG SBOM R&D effort

USAF Software SBOM R&D Efforts Collecting SBOMs

- Establishing a Hardware/Software stack (simulating a Space Force Weapon System stack) to collect SBOMs from firmware and software in the stack
  - Participating suppliers: undisclosed but you would recognize them
  - Establish SBOM processes



Mission Unique Software

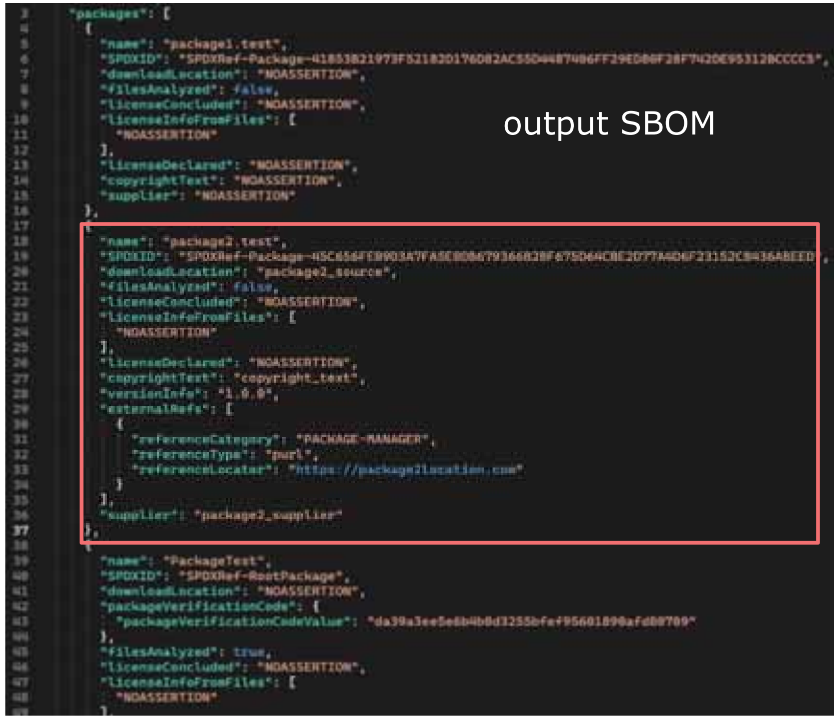
Real Time Operating System

Bare Metal Firmware

Hardware

USAF Software SBOM R&D Efforts Generating SBOMs

- Experimenting with SBOM generation tools
  - Microsoft SBOM Tool
    - Languages thus far: .Net, Python, C/C++, C#, Java, Ada

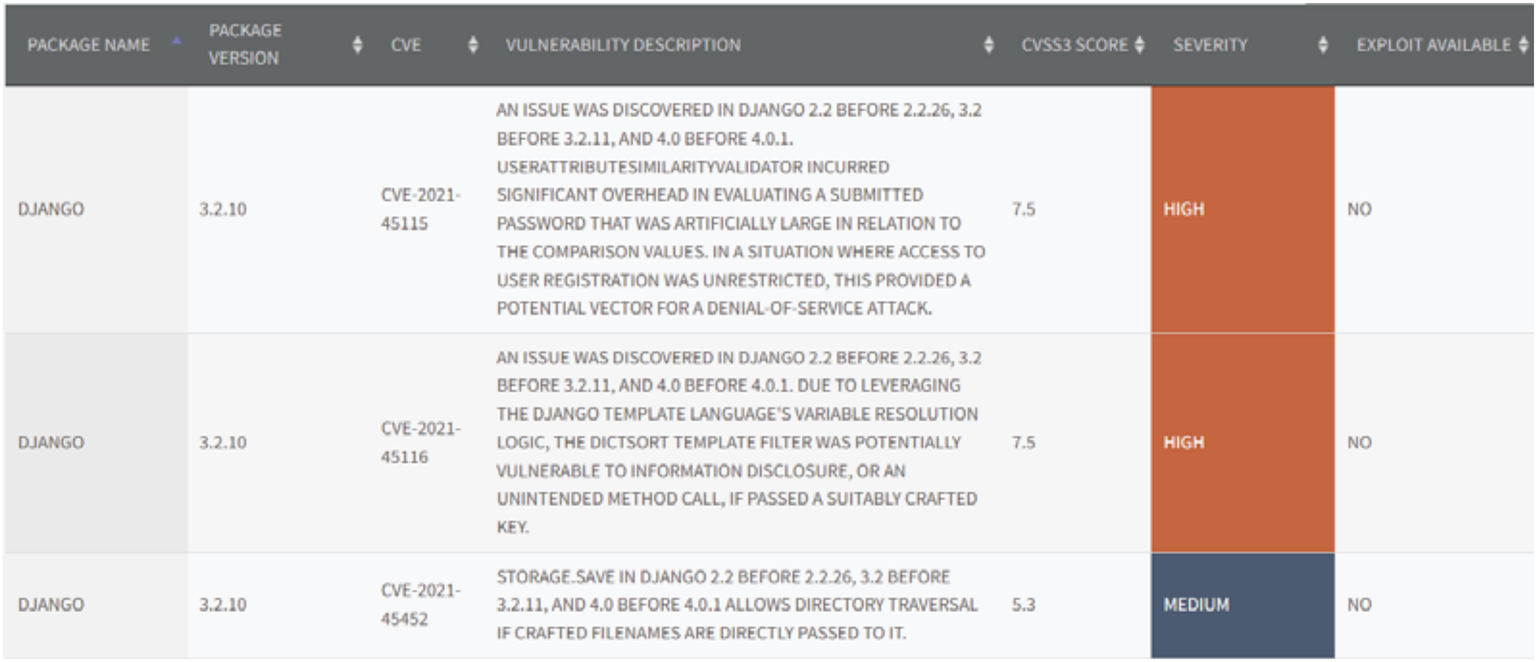


output SBOM

```
  "packages": [
    {
      "name": "package1.test",
      "SPDXID": "SPDXRef-Package-41853821973F52182D176D82AC55D4487496FF29ED86F28F7420E95312BCCCC5",
      "downloadLocation": "NOASSERTION",
      "filesAnalyzed": false,
      "licenseConcluded": "NOASSERTION",
      "licenseInfoFromFiles": [
        "NOASSERTION"
      ],
      "licenseDeclared": "NOASSERTION",
      "copyrightText": "NOASSERTION",
      "supplier": "NOASSERTION"
    },
    {
      "name": "package2.test",
      "SPDXID": "SPDXRef-Package-45C656FE89D3A7FA5E8D8679366828F675D64CBE2D77A4D6F23152C8436ABEED",
      "downloadLocation": "package2_source",
      "filesAnalyzed": false,
      "licenseConcluded": "NOASSERTION",
      "licenseInfoFromFiles": [
        "NOASSERTION"
      ],
      "licenseDeclared": "NOASSERTION",
      "copyrightText": "copyright_text",
      "versionInfo": "1.0.0",
      "externalRefs": [
        {
          "referenceCategory": "PACKAGE-MANAGER",
          "referenceType": "purl",
          "referenceLocator": "https://package2location.com"
        }
      ],
      "supplier": "package2_supplier"
    },
    {
      "name": "PackageTest",
      "SPDXID": "SPDXRef-RootPackage",
      "downloadLocation": "NOASSERTION",
      "packageVerificationCode": {
        "packageVerificationCodeValue": "da39a3ee5e6b4b0d3255bfef95601890afd80709"
      },
      "filesAnalyzed": true,
      "licenseConcluded": "NOASSERTION",
      "licenseInfoFromFiles": [
        "NOASSERTION"
      ],
```

USAF Software SBOM R&D Efforts Consuming (Analyzing) SBOMs

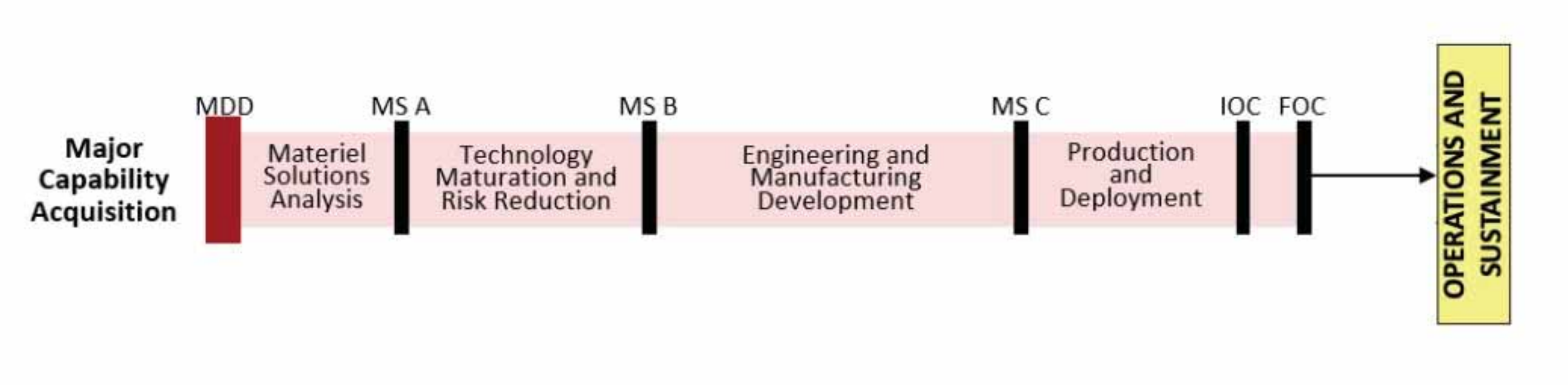
- **Experimenting with SBOM vulnerability identification tools (which use internet-based databases)**
  - **Daggerboard**
  - **OWASP Dependency Track**



PACKAGE NAME	PACKAGE VERSION	CVE	VULNERABILITY DESCRIPTION	CVSS3 SCORE	SEVERITY	EXPLOIT AVAILABLE
DJANGO	3.2.10	CVE-2021-45115	AN ISSUE WAS DISCOVERED IN DJANGO 2.2 BEFORE 2.2.26, 3.2 BEFORE 3.2.11, AND 4.0 BEFORE 4.0.1. USERATTRIBUTESIMILARITYVALIDATOR INCURRED SIGNIFICANT OVERHEAD IN EVALUATING A SUBMITTED PASSWORD THAT WAS ARTIFICIALLY LARGE IN RELATION TO THE COMPARISON VALUES. IN A SITUATION WHERE ACCESS TO USER REGISTRATION WAS UNRESTRICTED, THIS PROVIDED A POTENTIAL VECTOR FOR A DENIAL-OF-SERVICE ATTACK.	7.5	HIGH	NO
DJANGO	3.2.10	CVE-2021-45116	AN ISSUE WAS DISCOVERED IN DJANGO 2.2 BEFORE 2.2.26, 3.2 BEFORE 3.2.11, AND 4.0 BEFORE 4.0.1. DUE TO LEVERAGING THE DJANGO TEMPLATE LANGUAGE'S VARIABLE RESOLUTION LOGIC, THE DICTSORT TEMPLATE FILTER WAS POTENTIALLY VULNERABLE TO INFORMATION DISCLOSURE, OR AN UNINTENDED METHOD CALL, IF PASSED A SUITABLY CRAFTED KEY.	7.5	HIGH	NO
DJANGO	3.2.10	CVE-2021-45452	STORAGE.SAVE IN DJANGO 2.2 BEFORE 2.2.26, 3.2 BEFORE 3.2.11, AND 4.0 BEFORE 4.0.1 ALLOWS DIRECTORY TRAVERSAL IF CRAFTED FILENAMES ARE DIRECTLY PASSED TO IT.	5.3	MEDIUM	NO

USAF Software SBOM R&D Efforts
Notional SBOM Roles in a DoD Program

- 309 SWEG SCRM IPT
  - Developing roles and responsibilities for generation and distribution of SBOMs
  - Minimizing supply chain risks of ingested software


Major Capability Acquisition
MDD
MS A
MS B
MS C
IOC
FOC
Materiel Solutions Analysis
Technology Maturation and Risk Reduction
Engineering and Manufacturing Development
Production and Deployment
OPERATIONS AND SUSTAINMENT

Notional

	Prime	DoD Sw Dev	DoD PMO
Collect	x		x
Validate	x		x
Consume	x		x
Generate	x	x	
Distribute	x	x	

USAF Software SBOM R&D Efforts Notional SBOM Stakeholder Involvement

SBOM in a DoD Software Development Organization

- Policy
- DEVOPS
- Configuration Management
- Software Assurance
- Cybersecurity
- System Engineering
- Intelligence
- Enforcement
- Contracting & Acquisitions

Current Challenges with SBOMs

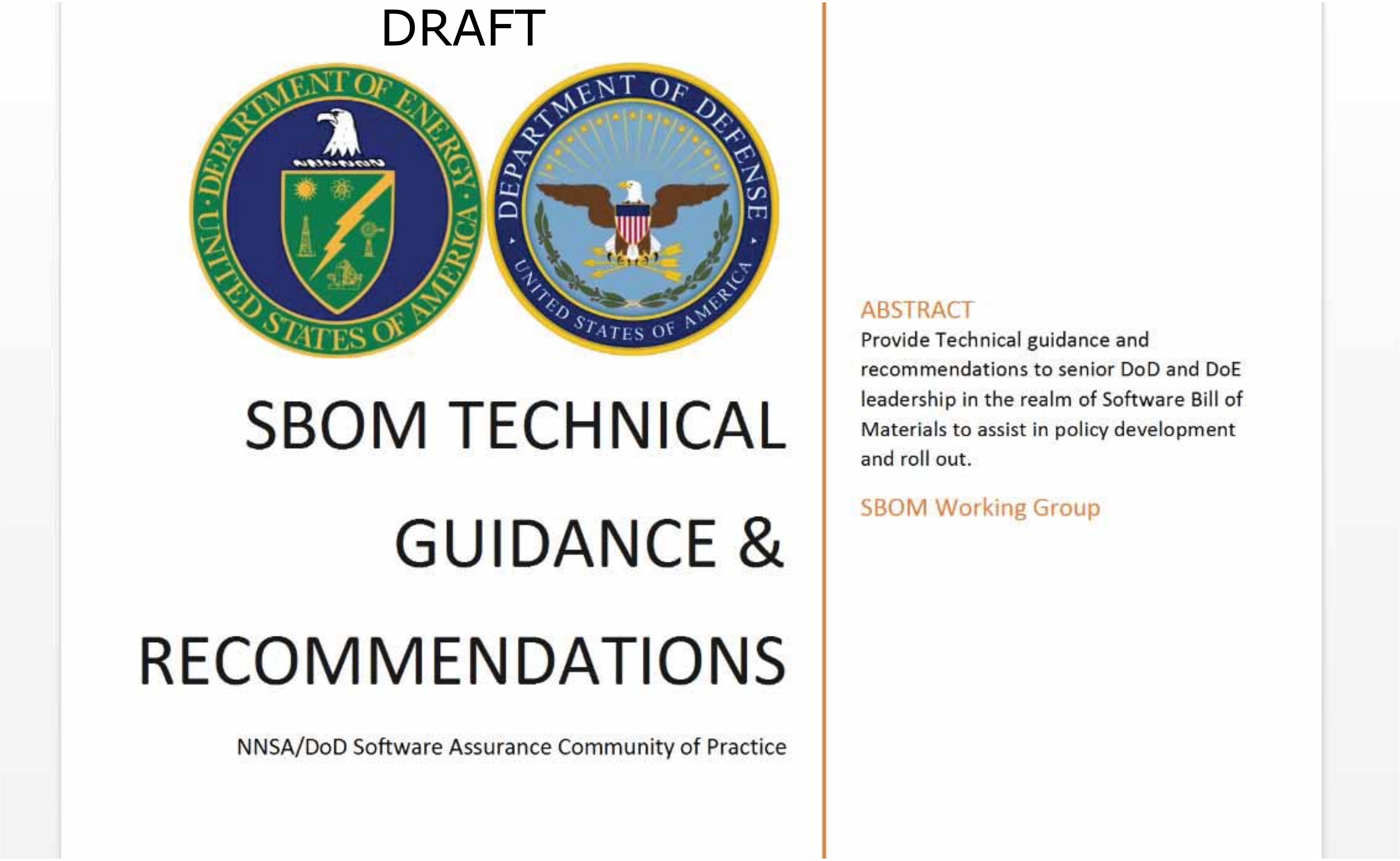
- No requirement, so few suppliers feel compelled to create them or request from their suppliers
- Disconnected networks will require database updates periodically
- A vulnerability of a software component on an unclassified system often becomes classified, thus requiring special handling
- Suppliers may deem their software proprietary thus limiting access to build-version SBOMs
- Where do we store SBOMs? Who has access? How often do we receive them?
- Who has ultimate responsibility for collection, validation, consumption (analysis) of SBOMs? DoD, Services, PMOs?
- …

DoD/NNSA Software Assurance CoP SBOM WG Update

DoD/NNSA SwA CoP SBOM WG Update

- Team: OSD R&E, MITRE, Aerospace, SEI, DHS/CISA, NNSA, MDA, and the Services
- Effort kicked off at December 2022 SwA CoP
- USAF Software Directorate appointed as lead
- Expecting V1.0 publication in March 2024
- Tasks:
  - Develop a white paper during CY2023 on the SBOM processes and policies needed for both DoD and DoE
    - Provide short-lead policy input during the paper development as requested

DRAFT



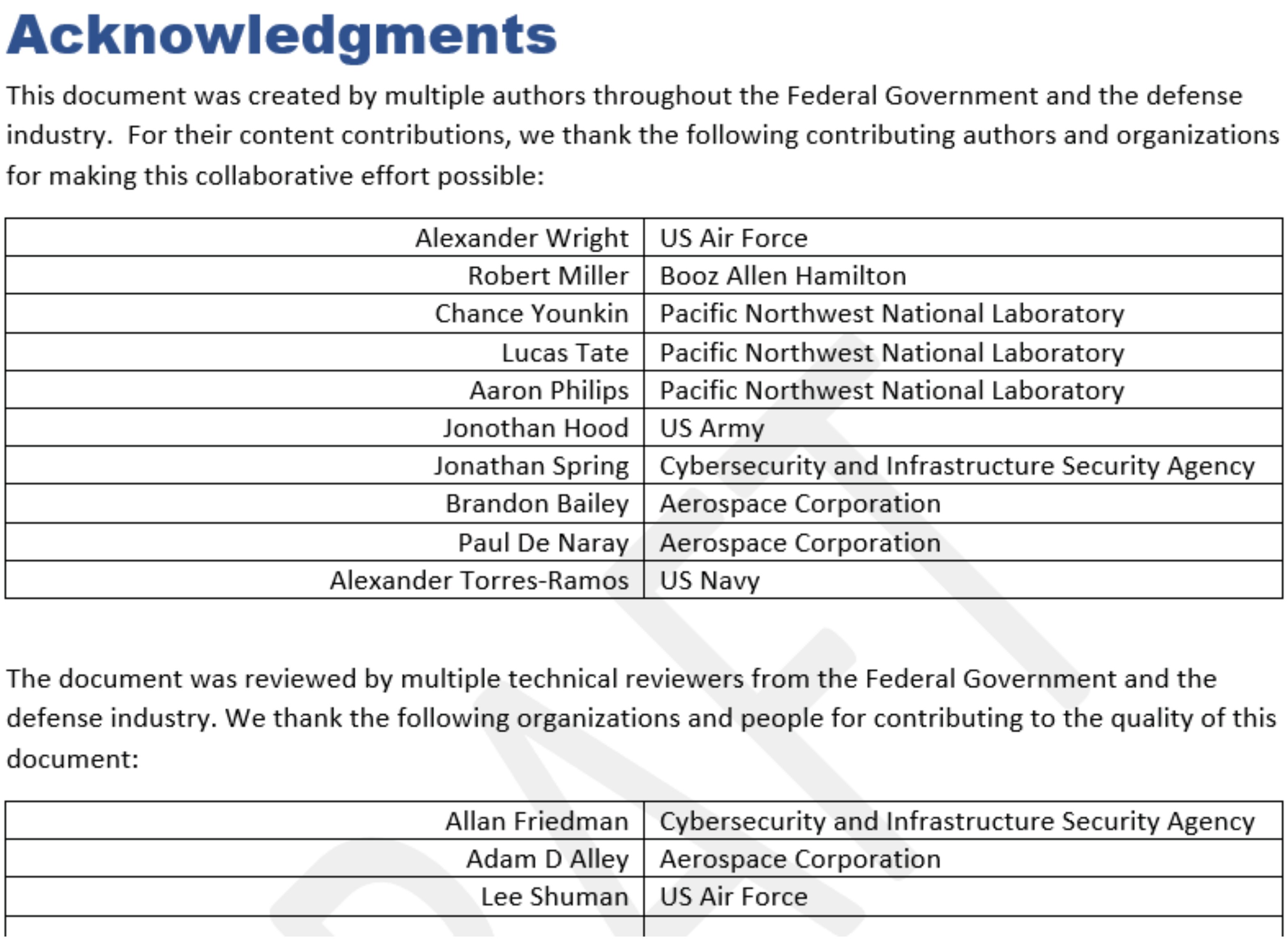
SBOM TECHNICAL GUIDANCE & RECOMMENDATIONS

NNSA/DoD Software Assurance Community of Practice

ABSTRACT

Provide Technical guidance and recommendations to senior DoD and DoE leadership in the realm of Software Bill of Materials to assist in policy development and roll out.

SBOM Working Group



Acknowledgments

This document was created by multiple authors throughout the Federal Government and the defense industry. For their content contributions, we thank the following contributing authors and organizations for making this collaborative effort possible:

Alexander Wright	US Air Force
Robert Miller	Booz Allen Hamilton
Chance Younkin	Pacific Northwest National Laboratory
Lucas Tate	Pacific Northwest National Laboratory
Aaron Philips	Pacific Northwest National Laboratory
Jonothan Hood	US Army
Jonathan Spring	Cybersecurity and Infrastructure Security Agency
Brandon Bailey	Aerospace Corporation
Paul De Naray	Aerospace Corporation
Alexander Torres-Ramos	US Navy

The document was reviewed by multiple technical reviewers from the Federal Government and the defense industry. We thank the following organizations and people for contributing to the quality of this document:

Allan Friedman	Cybersecurity and Infrastructure Security Agency
Adam D Alley	Aerospace Corporation
Lee Shuman	US Air Force

Table of Contents #1

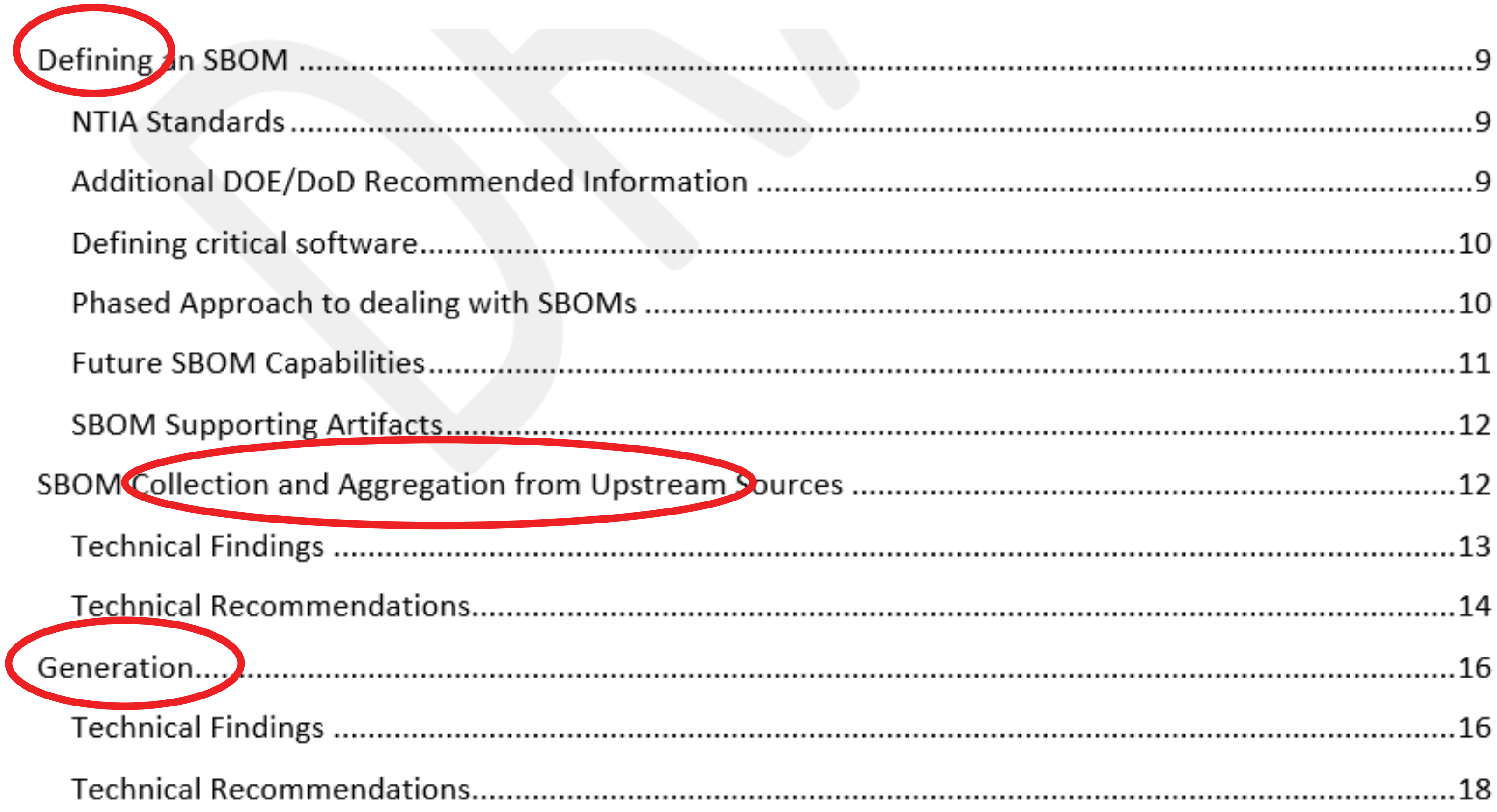


Table of Contents #2

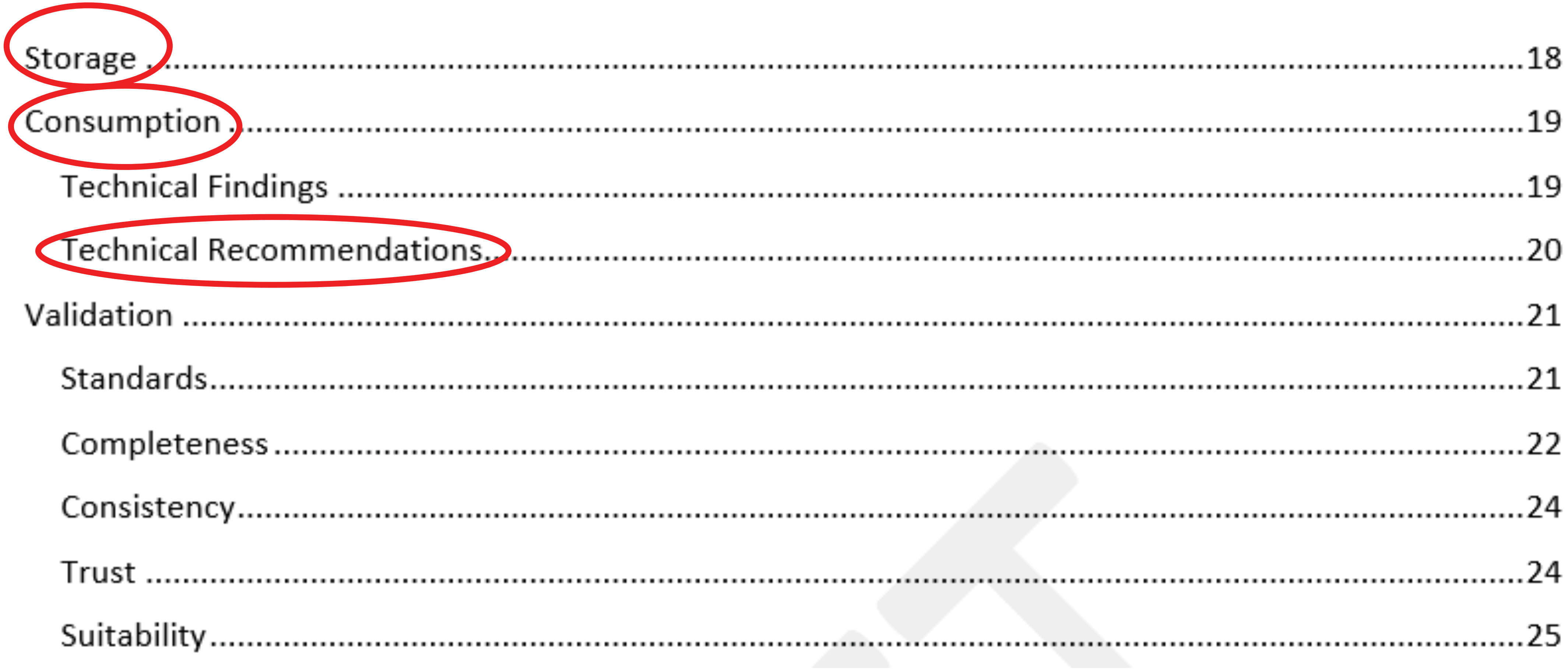
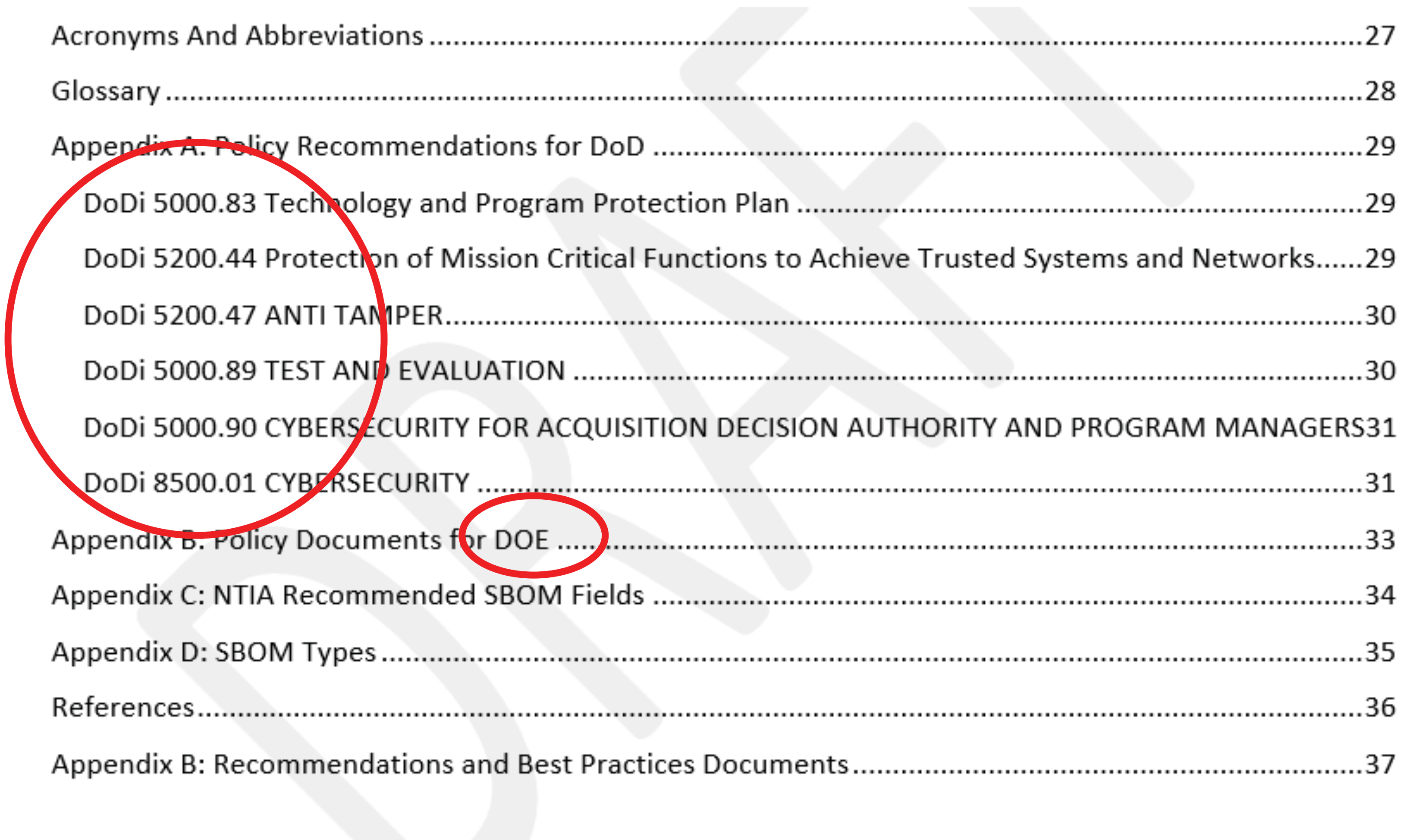
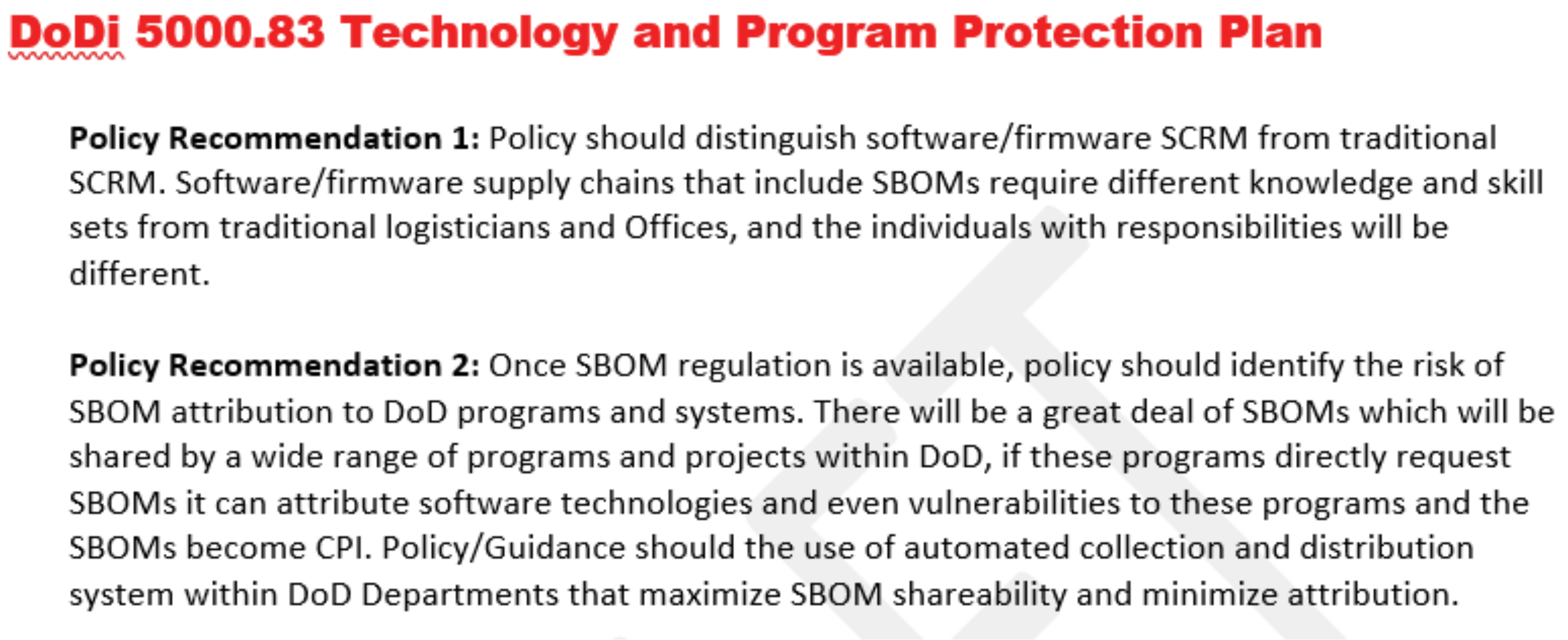


Table of Contents 3



Appendix A: Policy Recommendations for DoD #1

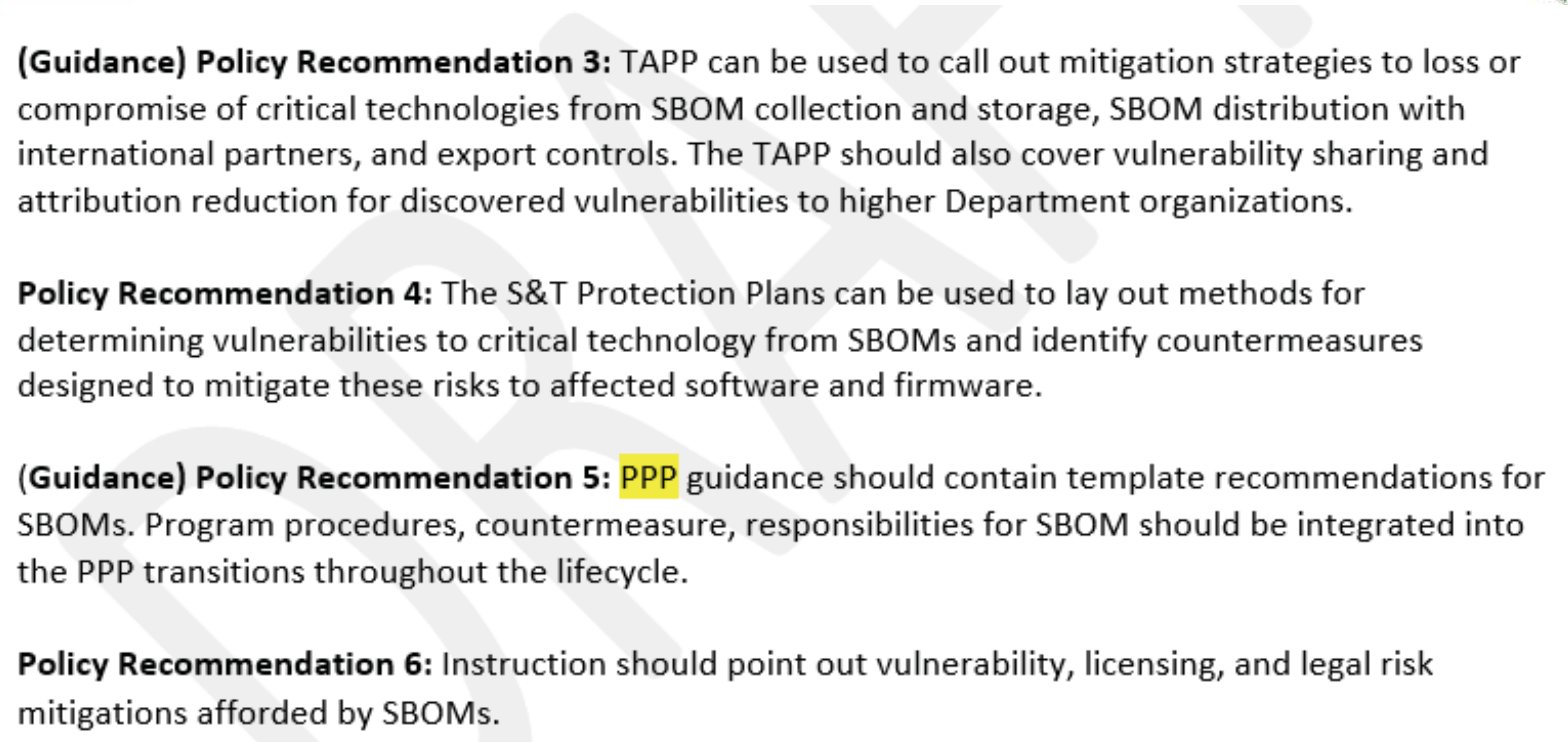


DoDi 5000.83 Technology and Program Protection Plan

Policy Recommendation 1: Policy should distinguish software/firmware SCRM from traditional SCRM. Software/firmware supply chains that include SBOMs require different knowledge and skill sets from traditional logisticians and Offices, and the individuals with responsibilities will be different.

Policy Recommendation 2: Once SBOM regulation is available, policy should identify the risk of SBOM attribution to DoD programs and systems. There will be a great deal of SBOMs which will be shared by a wide range of programs and projects within DoD, if these programs directly request SBOMs it can attribute software technologies and even vulnerabilities to these programs and the SBOMs become CPI. Policy/Guidance should the use of automated collection and distribution system within DoD Departments that maximize SBOM shareability and minimize attribution.

Appendix A: Policy Recommendations for DoD #2



(Guidance) Policy Recommendation 3: TAPP can be used to call out mitigation strategies to loss or compromise of critical technologies from SBOM collection and storage, SBOM distribution with international partners, and export controls. The TAPP should also cover vulnerability sharing and attribution reduction for discovered vulnerabilities to higher Department organizations.

Policy Recommendation 4: The S&T Protection Plans can be used to lay out methods for determining vulnerabilities to critical technology from SBOMs and identify countermeasures designed to mitigate these risks to affected software and firmware.

(**Guidance) Policy Recommendation 5:** PPP guidance should contain template recommendations for SBOMs. Program procedures, countermeasure, responsibilities for SBOM should be integrated into the PPP transitions throughout the lifecycle.

Policy Recommendation 6: Instruction should point out vulnerability, licensing, and legal risk mitigations afforded by SBOMs.

DoD/NNSA SwA CoP SBOM WG Summary

- Publish SBOM Technical Guidance and Recommendations V1.0 in March 2024
- Publish annual updates and add appendices as SBOM policy and implementation of them matures
- Continue to provide short-lead policy input as requested

Contact Us

- **Parker Bauer**
  - parker.bauer@us.af.mil
  - (801) 777-5308
- **Alexander Wright**
  - alexander.wright.4@us.af.mil
  - (720) 648-8694

Discussion