309 SWEG Supply Chain Risk Management
Software Support Center

USAF C-SCRM/SBOM

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
- Q&A

Background

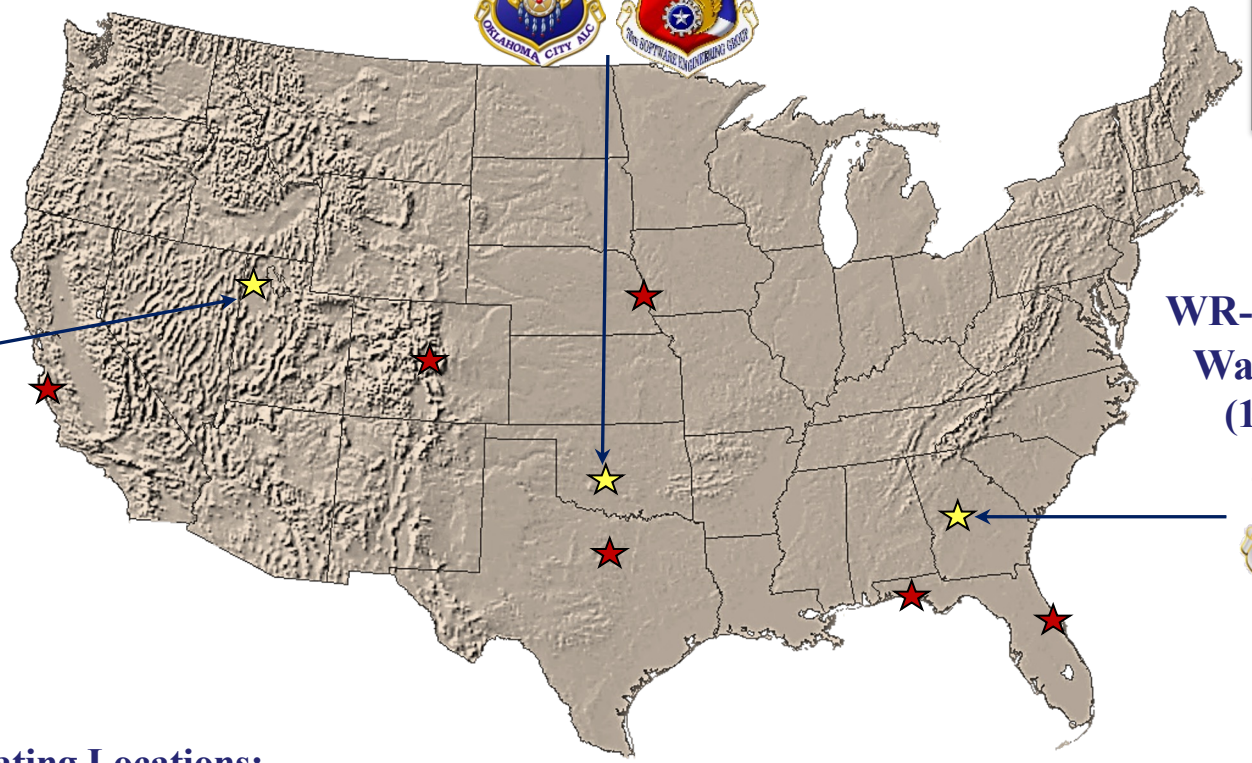
Background
USAF Software

~4,500+ Software Professionals Combined

OC-ALC, Tinker AFB
Oklahoma City, OK
(1300+ Personnel)

Specializing in Operational Programs, C4I, Mission Support, Test Program Sets and Training Systems

OO-ALC, Hill AFB
Ogden, UT
(1900+ Personnel)

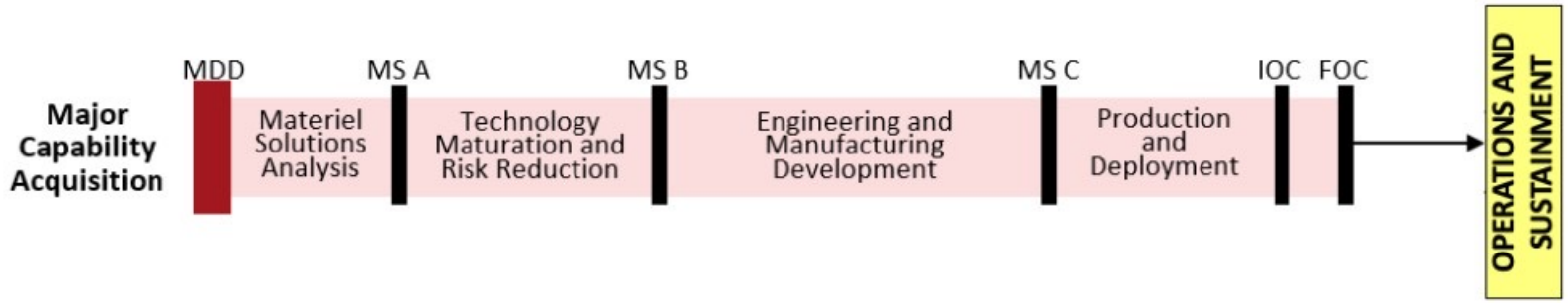


WR-ALC, Robins AFB
Warner Robins, GA
(1300+ Personnel)

★ Six (6) Current Operating Locations:
Vandenberg AFB, CA – Peterson AFB, CO – NAS-JRB, TX – Offutt AFB, NE – NAS Pensacola, FL – Patrick AFB, FL

Background
USAF Software Traditional Role

Acquisition Lifecycle Phases



FOC

Sustainment Phase

Develop Software and Firmware

New Capability Integrated into Weapon Systems

Add Code to Software and Firmware

Primes

USAF, USA, USN software

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
Assistant Inspector General
Acquisition, Contracting, and Sustainment

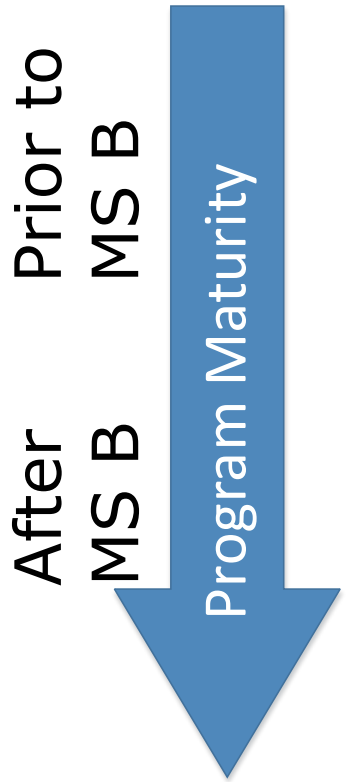
~~FOR OFFICIAL USE ONLY~~

DODIG-2018-143 | 9

Background
AFSPC C-SCRM Effort

- **Enterprise Ground Services (EGS)**
  - **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 software expertise**

On-Site Technical Supplier C-SCRM Assessments When?



Intelligence Reports

Business Analytic Reports

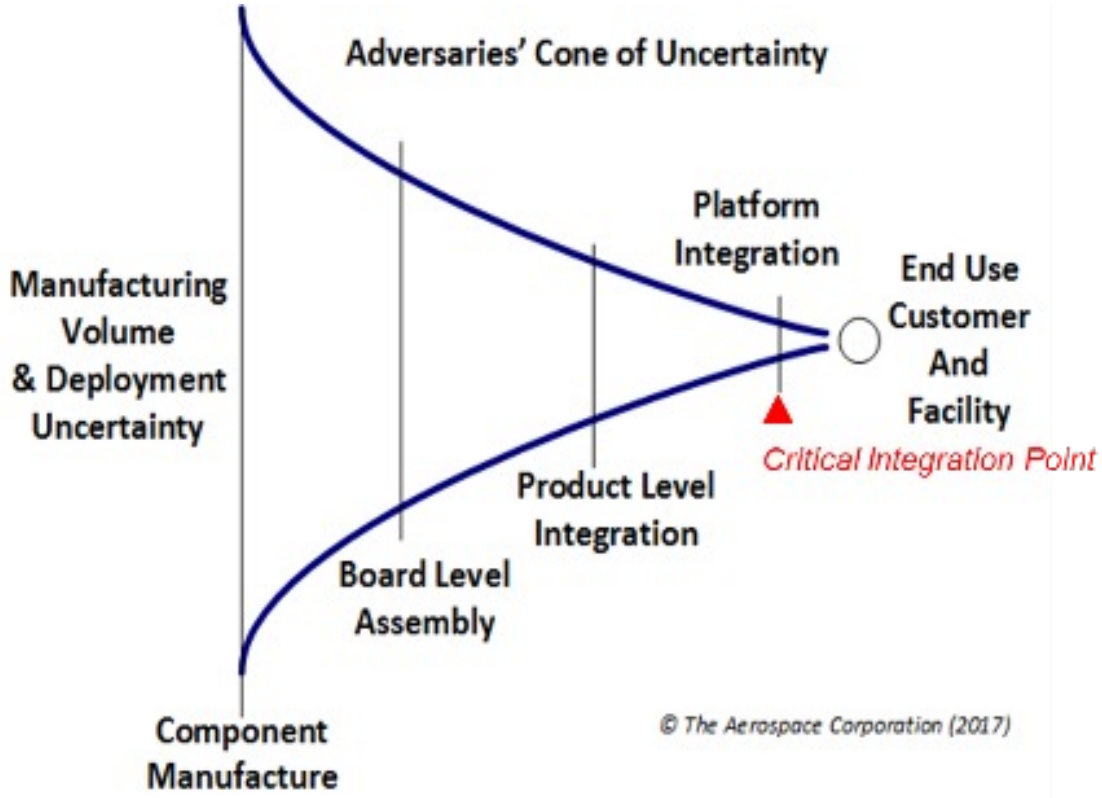
Technical Field C-SCRM Assessments

Pre-Procurement

Traditional Assurance Practices

Post-Procurement

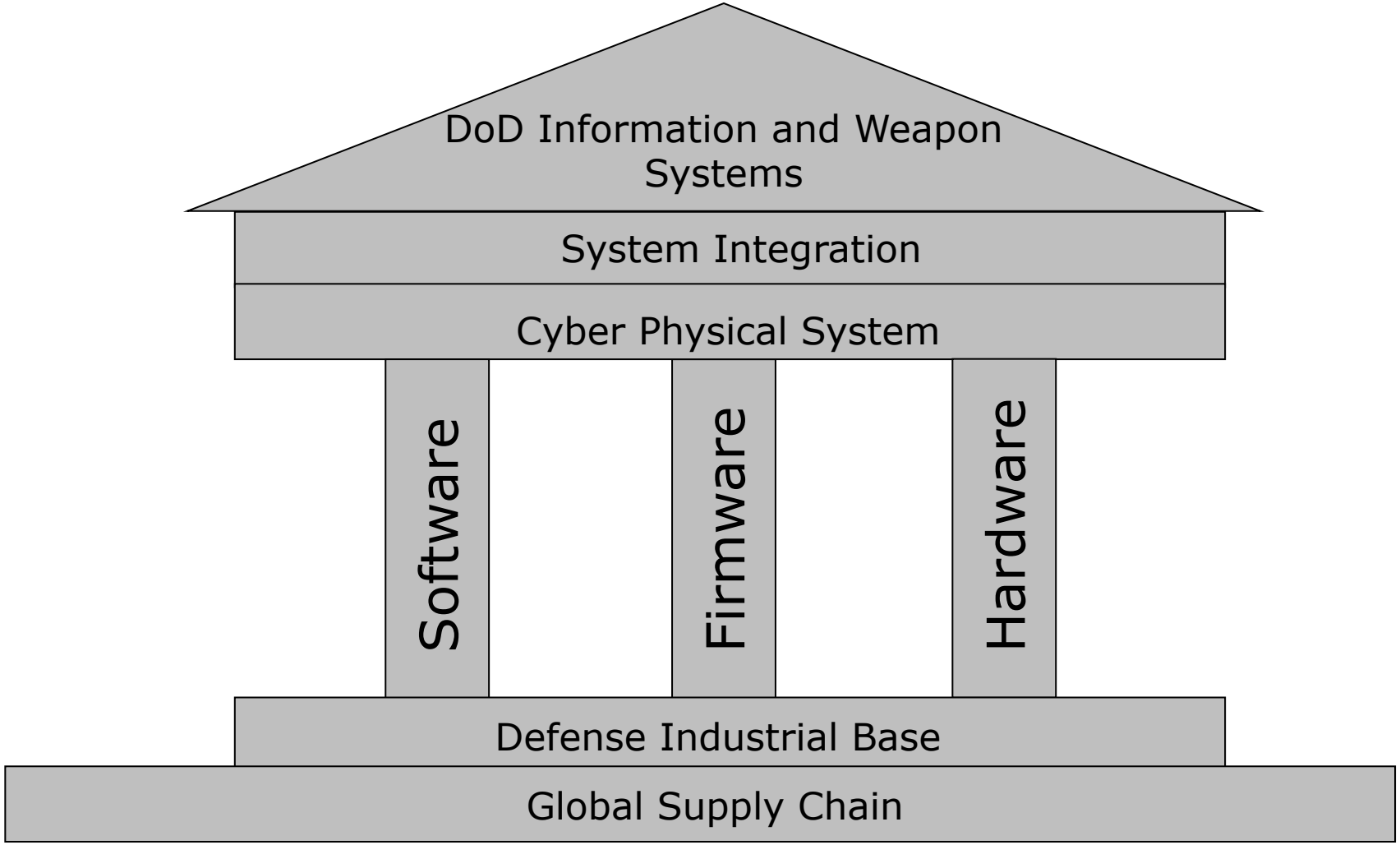
On-Site Technical Supplier C-SCRM Assessments
Which Suppliers?



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
  - Observe dedicated DoD or USG development and integration facilities to understand cyber posture
  - Also allows for follow-up for improvement
- Private sector companies perform intrusive audits for multiple purposes – financial, quality, etc. Do 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?

- General Organizational 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?

Observations are rated by risk level and compiled by category.

Category	L0	L1	L2	L3
General				
Organizational SCRM Practicies		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.**
- **Additional risks are also documented.**

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

On-Site Technical Supplier C-SCRM Assessments Summary

- Another tool for DoD programs to assess and reduce supplier risks
- Suppliers to date have welcomed the results as it has helped them improve their risk posture
- Best 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

- **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 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**

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

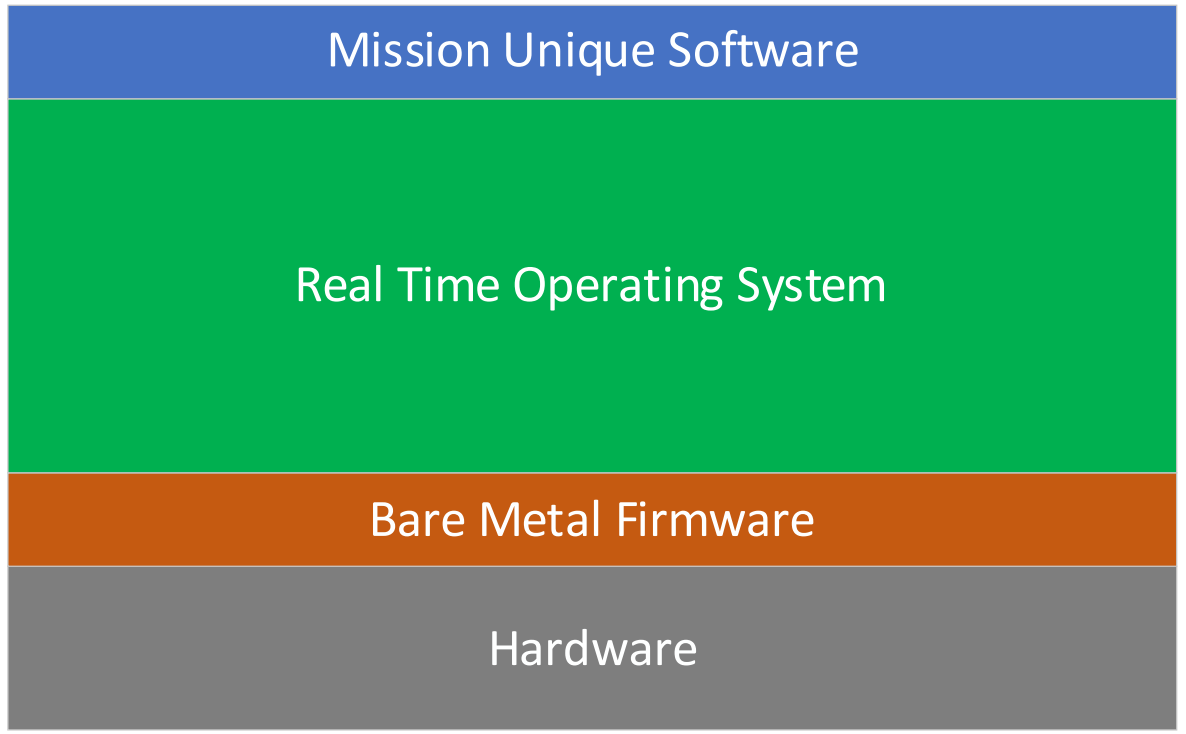
USAF Software SBOM R&D Efforts Effort Summary

- 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
- Timeline for 309 SWEG SBOM R&D effort

Collect/Validate

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**



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
  - SwiftBOM (CERT)

output SBOM


```
"packages": [
  {
    "name": "package1.test",
    "SPDXID": "SPDXRef-Package-41853B21973F52182D176D82AC55D4487406FF29ED80F28F742DE95312BCCCC5",
    "downloadLocation": "NOASSERTION",
    "filesAnalyzed": false,
    "licenseConcluded": "NOASSERTION",
    "licenseInfoFromFiles": [
      "NOASSERTION"
    ],
    "licenseDeclared": "NOASSERTION",
    "copyrightText": "NOASSERTION",
    "supplier": "NOASSERTION"
  },
  {
    "name": "package2.test",
    "SPDXID": "SPDXRef-Package-45C656FE09D3A7FA5E0DB679366B2BF675D64CBE2D77A4D6F23152C8436ABEED",
    "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

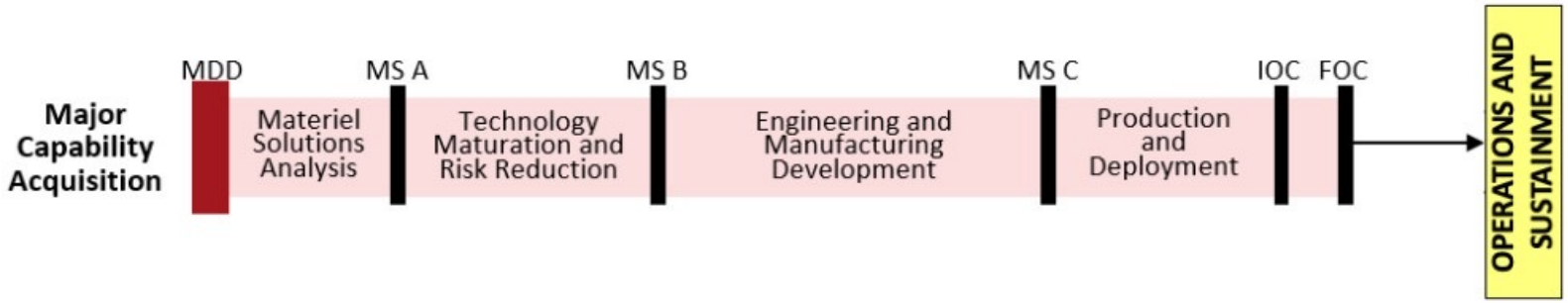
USAF Software SBOM R&D Efforts
Notional SBOM Swim Lanes

SBOM in a DoD Sw Dev Org

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

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**



Notional

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

Current Challenges with SBOMs

- No requirement so few suppliers feel compelled to create them or request from their suppliers
- Disconnected networks will require databases updated periodically
- A vulnerability of a software component on an unclassified system often becomes classified requiring special handling
- Suppliers may deem their software proprietary thus limiting access to build-version SBOMs
- Where do we store SBOMS?
- Who has ultimately responsibility for collection, validation, consuming (analyzing) 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, National Labs, MDA, and the Services
- Effort kicked off at December SwA CoP
- USAF appointed as lead
- 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
  - Review and provide input to the SBOM Style Guide v0.1
    - Initiated in OSD XBOM WG
    - Additional input forthcoming as we adapt it from white paper (see below)

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

Contact Us

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

Discussion