Global Supply Chain Security for Microelectronics

Secure Design Session Report Out – July 29, 2022

27 – 29 July 2022 workshop

Secure Design Session

FACILITATOR

Daniel Radack
Institute for Defense Analyses (IDA)

Supported by the following organizations:

OUSD(A&S) DMCFT	BAE Systems / JEDEC
Defense Logistics Agency Land and Maritime	The Open Group
Aerospace Corp.	Qualcomm
Tenet3	Cisco
Collins Aerospace	Huntington Ingalls Industries (HII)
ANSI	Defense Standardization Program Office
Boeing	Aerospace Engineering Solutions International
Siemens Government Technologies	Integrity Security Services
Booz Allen Hamilton	Private
Raytheon Technologies	Battelle
Semiconductor Industry Associatio	IEEE
Synopsys Inc	Cinch
NIST	NAVSEA
CloudPosition	SAE Industry Technologies Consortia
NASA	OSD(R&E), Critical Technologies, Microelectronics
Bowhead Cybersecurity Solutions and Services	GlobalFoundries Inc.
Air Force Research Lab	Telecommunications Industry Association (TIA)
Institute for Defense Analyses (IDA)	Microsoft

Breakout Question # 1a

What recommendations do you have regarding standards or sets of standards that provide ***commercially viable mitigations in support of FY20 NDAA Section 224 requirements***?

Areas Identified:

- More effort needed to develop a more complete matrix of existing standards and how they map into design and lifecycle microelectronics
- Viability, the industry buy-in to fill in gaps, rich discussion, however need even more industry discussion
- Other industries have standards: medical, safety & critical, automotive, aerospace; but cost considerations need to be factored if use these standards
- No obvious plug and play solution

Breakout Question # 1b

What recommendations do you have regarding standards or sets of standards that provide ***coverage across all phases of the microelectronics development lifecycle?***

Areas Identified:

- Some pieces of each standard may apply; challenge is how to pull “pieces” into complement of standards, more of a framework
- Values of overarching standards and more focused industry standards
- Standards don’t address all of 224, need to drill down more into specifics, like threats
- Some other industry standards may be applicable, but not mapped, so would need to have thorough review. Have not seen one solution.

Breakout Question # 1c

What recommendations do you have regarding standards or sets of standards that provide ***coverage across vendor types (system integrators, original equipment manufacturers, component distributors, original component manufacturers)?***

Areas Identified:

- Contention/discussion – greatly benefit from more commercial suppliers
- Commercial companies need to innovate and use global assets
- Discussed how some standards could be equally applied across COTS and foundries – look broadly or pick specific problem to solve.
- Further refinement in design process to determine in standards matrix how standards could implement 224 requirements

Standards Identified – Secure Design

1. ISO/IEC 20243-1:2018: Information technology — Open Trusted Technology Provider TM Standard (O-TTPS) — Mitigating maliciously tainted and counterfeit products — Part 1: Requirements and recommendations – Particularly lifecycyle and secure engineering
2. IPC-1791: Trusted Electronic Designer, Fabricator and Assembler Requirements
3. Accelera IP Security Assurance Working Group https://accellera.org/downloads/standards/ip-security-assurance
4. RTCA DO-254
5. EASA CM – SWCEH – 001
6. ISO 26262

Breakout Question #2a

What suggestions do you have for DoD to improve its candidate standards approach in terms of ***the modular approach for integrated assured supply chain***?

Areas Identified:

- Not step function. Smaller goals that lead to bigger picture
- Embraced by industry

Breakout Question #2b

What suggestions do you have for DoD to improve its candidate standards approach in terms of ***what methods would you suggest for determining and sharing compliance to standards across supply chain and to acquirer***?

Areas Identified:

- DoD should not be the compliance agent
- If decided to pull a “piece of a standards”, compliance may be lost, so may not be best solution

Breakout Question #2c

What suggestions do you have for DoD to improve its candidate standards approach in terms of ***what section 224 related factors influence sub-tier vendor selection***?

Areas Identified:

- Discussion of demographics listed in 224. More discussion needed on real threat is and advantage of including this in a standard and organizations complying with standard. Need better understanding of what artifacts would be needed to meet demographics.
- Define threats and mitigation of such.

Breakout Question #2d

What suggestions do you have for DoD to improve its candidate standards approach in terms of ***requirements development and flow down***?

Areas Identified:

- Overarching standard vs industry specific

Breakout Question #2e

What suggestions do you have for DoD to improve its candidate standards approach in terms of **DoD adoption strategy and timelines**?

Areas Identified:

- Not to use step function
- Small victories
- Pilot projects
- Determine what can do immediately (things that exist) and other longer term filling of the gap in areas that need consensus, that haven’t been achieved as of yet

Breakout Question #2f

What suggestions do you have for DoD to improve its candidate standards approach in terms of ***DoD organization of standards***?

Areas Identified:

- Recognize need to get procurement and acquisition involved and their buy in

Breakout Question #3

What are the top 2-3 most important take-aways from the discussions in your breakout group?

Areas Identified:

1. DoD – could support pilot programs that would support this incrementally
2. Threats and mitigations more thoughtfully considered and filing gaps with new standards. Even over arching standard needs threat analysis
3. Data – what are we collecting? How used? Artifacts of data? Government could encourage standards in this area
4. Addressing CIA is too high level, define what we mean at the design level – traceability, provenance, risks, quality, validation – all need definition
5. Balance of near term vs. long term