Global Supply Chain Security for Microelectronics

Information and IP Protection Session Report Out– October 28, 2022

26 – 28 October 2022 workshop

Information & IP Protection Session

FACILITATOR
Donald Davidson
Synopsys

Supported by the following organizations:

Aerocyonics, Inc.	Intrinsix Corp
Aerospace Corp.	LH SMC Metal, LLC
Amazon Web Services (AWS)	National Institute of Standards and Technology (NIST)
CALCE	Parenteral Drug Association® (PDA)
Cisco	Qorvo
Collins Aerospace	Sandia National Laboratories
DMEA	Tenet3
DoD R&E	The Charles Stark Draper Laboratory Inc.
Georgia Tech Research Institute	The MITRE Corporation
Global Operations - Advanced Sourcing	UL Solutions
Hewlett Packard Enterprise	West Virginia University
HII	Wikitechnium LLC
Intel Corporation	Woodward, Inc.

Q4a Key Takeaways – Information Protection/Confidentiality of Data

What candidate considerations were discussed and what were the key takeaways?

1. Most COTS do not have a specific agreement for confidentiality in either direction – acquirer or supplier (confidentiality may be addressed in a trusted supplier relationship or additional contract language).
2. Most COTS products are bought from distributors rather than the OEMs. Public data sheets may reflect technical and compliance information on the product, not on the process for design and FAB. (Additional product information would have to be sought through the OEM.)
3. Acquirer confidentiality can be somewhat afforded through blind buys (but blind buys limit reachback capability to OEMs).

Q4a Key Takeaways – Design for Data Security

What candidate considerations were discussed and what were the key takeaways?

1. Security capability of the COTS device. Secure Boot, Hardware Root of Trust, PUFs.
2. Knowing how to do the security provisioning and knowing what has already been done is an important feature. (Usually found in technical reference manuals (TRMs) or application notes.)
3. How to use the security features: key lengths, key algorithms. And redundancy of security features.

Q4a Key Takeaways – Data Requirements

What candidate considerations were discussed and what were the key takeaways?

1. What is needed to make secure procurement decision:

- Who is the company and where is product designed?
- Where product was Fabbed?
- Where was it packaged?
- Date of assembly
- Who did assembly?
- Was anything outsourced and if so, to whom?

2. Risk-based decisions may be informed by SBOM or HBOM

Q4a Key Takeaways – Chain of Custody

What candidate considerations were discussed and what were the key takeaways?

1. All the supply chain categories were valid. In addition:

- Ø What was the final path to the distributor?
- Ø Are there item-unique identifiers and how do they track them?

LOA: A

- **Ideally highest level assurance products will be designed and manufactured in U.S. or Allied countries. (“In-country diffusion.”)**

- **Information Protection:** Acquirer data is protected in accordance with NIST SP 800-172 or DCSA certification; Compatible standard for Supplier data (ISO 27001 or similar); Information assurance and data security practices.

- **Design for Data Security:** Do they have secure keys, encryption, role-based access, encryption (and identify – Suite B at minimum), SBOM, multiple redundant security paths?

Trusted 3rd party attestation/certification that netlist matches design specification. An external audit would allow for this to remain in the COTS space.

- **Data Availability:** *Custom*: Identify design house, Fab, Process used, Who packaged, locations of all phases, who and how shipped and ideally dates.
  - *COTS*: Country of diffusion and country of origin with
    1. Documented procedures; auditable; how is audit trail maintained and how long is it maintained?
    2. Suppliers have data readily available and are willing to provide it without a contract.

- **Chain of Custody:** Some manufacturers have serial numbers, Item Unique Identifier (IUD), PUF. Path to the distributor. Visibility at all Tier 1s and dig deeper on other components. Verify coming from U.S.-friendly countries.

LOA: B

- **Information Protection:** NIST SP 800-171 (CMMC levels to be determined).
- **Design for Data Security:** Multiple security features. Do they have secure keys, encryption (FIPS 140-2 or 3), role-based access, SBOM.
- **Data Availability:** Country of diffusion and Country of origin.
- **Chain of Custody:** Visibility into critical Tier 1 components. Path to the distributor.

LOA: C & D

Not addressed

Q4c Key Takeaways:

What areas demonstrated the greatest need in terms of relevant regulations, policy, standards, best practices?

1. Data availability (SBOM may help)
2. Data delivery standardization, format, etc.
3. No standard for business intelligence on supply chain

Q4e Key Takeaways:

What recommendations does the group have for DoD on next steps for section 224?

1. Develop a pilot use case using Section 224 identified standards including cost-benefit analysis.
2. Where are there gaps?
3. What SDOs might be leveraged to fill those gaps?
4. Who in U.S. government or industry might lead a standards initiative?

Additional References

- ISO 26262 Functional Safety Standard
- IEC 61508 Overview – Functional Safety in Industrial Manufacturing
- IEC 61511 Functional Safety
- ISO 27036 Cybersecurity – Supplier Relationships
- NIST SP 800-171 Assessment for DoD Contractors
- NIST SP 800-172 Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171
- IPC-2591 CFX Standard – Connected Factory Exchange - https://www.ipc.org/ipc-cfx (a start)
- Hardware Root of Trust
- NIST FIPS 140-2
- Accellera Systems Initiative: IP Security Assurance Standard Whitepaper

Questions / Discussion?