Global Supply Chain Security for Microelectronics

Procurement Management Session Report Out – July 29, 2022

27 – 29 July 2022 workshop

ANSI

Procurement Management Session

FACILITATOR
Lori Gordon
The Aerospace Corporation

- Intel
- Locusview
- Aerospace Corp
- Golden Altos
- Hewlett Packard
- US Partnership for Assured Electronics
- Aerocyonics
- IPC
- Defined Business Solutions
- Electronic Components Industry Assn
- GlobalFoundries
- Maxar Technologies
- Synopsys
- Booz Allen Hamilton
- DoD and SAIC/DMCFT
- Qualcomm
- HII
- General Atomics Aeronautical Systems
- ANSI
- Performance Review Institute
- The Open Group
- NASA & NASA GSFC
- NIST
- TTI
- Amazon
- Aerospace Industries Assn
- CALCE, Univ of MD
- Siemens DSW
- DUST Identity
- Hodgkins Consulting

What Workshop Outcomes Do You Want To See?

- Understand where the standards needs are for microelectronics (ME)
- Gauging feedback from community, systems engineering, program management
- We run counterfeit avoidance accreditation side - understand the conformity assessment (CA) side
- Listen and learn. Understand the challenges
- How can we leverage standards that already exist so we don't reinvent wheel
- What do we consider an adequate baseline for NDAA FY20 section 224?
- Share what we do - how can we support DoD
- Standards that offer flexibility to adopt COTS components
- Have a defined roadmap that is DoD supported and can be relied upon. There won't be one standard
- Systems engineering: An evaluation of risk associated with components installed (software/hardware)
- Technology – a trust anchor – to marry physical objects to digital thread (i.e., trusted cloud, distributed blockchain)

Desired Outcomes (contd.)

- What is public versus private data? What can be certified?
- Establish/understand data flow. Who needs it most/least? Build a community that shares data.
- Industry historically has not been transparent. How do we make data discoverable?
- What data? Is it an audit? That is do-able. Do your suppliers have a business continuity plan? That is actionable. What does the secure concept really mean?
- Better continuity between identity of parts and those that are chosen by procurement office. There is sometimes a disconnect. Different manufacturers have different part numbers.
- Tracking lifecycle in my distribution chain. Requires data flow
- Trusted chain of custody, validated transactions. Which standards do we look at?
- Hear thoughts on what a common baseline would look like
- What vendors you should select from a demographic perspective

Desired Outcomes (contd.)

- Identify standards, leverage existing standards, come up with a uniform approach
- Standards that help identify counterfeit parts in the supply chain
- Evaluation of risk, data management, traceability both physical and digital
- Consistency in supplier flow down
- Expectations of suppliers, supplier visibility
- Learn what other industries are doing
- Link between digital and physical world
- Link goals at national level for supply chain traceability and individual goals of end users
- We have a supplier risk assessment framework: U.S. Partnership for Secured Electronics members must be certified to IPC 1791 within one year of joining

Desired Outcomes (contd.)

- Look to larger companies to help shape best practices (“reputational trust”)
- Consider also challenges faced by small/medium sized companies and burden that framework might impose on them
- Hearing initial thoughts on standards, and value / business case of standards and widespread adoption of them
- Difference between trustworthiness and trust
- On top of existing standards are processes w/in industry. We have Trustparts database at component level. Helps with risk assessment. Having a standard that establishes trust would be good e.g. ISO 9000 has been tailored for aerospace
- We have to meet regulatory requirements flow downs. Right now it’s a patchwork. We don’t have a clear risk assessment approach for supply chain security. A lot of info out there that isn’t yet captured in standards
- There’s a vast amount of data generated by manufacturers. Who bears the burden for the costs to store it? Manufacturer or DoD?
- How should data be utilized / handled in an appropriate manner

Desired Outcomes (contd.)

- Come up with a way to more equitably distribute risk in the supply chain
- A COTS assemblies checklist has been developed to help with decision-making
- Open Group standard may be applicable. Understand how providers are giving input to procurement process
- Want to understand risk that section 224 is trying to address. There are standards that address forced labor. Some in ISO. Our weakness may be in trying to address newer risks in last few years. Counterfeit is long-term risk.
- How do we apply U.S. centric risk to companies that are global? Understand depth of the threat
- What is the on ramp and timeframe for full implementation?
- When we buy COTS is when it gets dangerous. Evaluate what is out there. How can we protect ourselves to increase the use of commercial parts?
- We have to meet SCRM requirements. Important to assign risk categories to parts.

Standards Recommendations

- There is no general standard that governs the supply chain. Many standards across SDOs.
- Mission Assurance Improvement Workshop documents
- COTS Assembly Checklist developed by Parts Management Working Group found here: https://www.dau.edu/cop/PMKSP/Lists/COTS_Checklist/AllItems.aspx
- Cybersecurity Maturity Model Certification (CMMC)
- SAE has developed a counterfeit parts roadmap
- Systems engineering, software assurance hardware assurance being covered by SAE G-32
- SAE JA7496 - Cyber Physical Systems Security Engineering Plan (CPSSEP)
- SAE JA6801 - Cyber Physical Systems Security Hardware Assurance in development (covers all phases of ME lifecycle, all vendor types)
- Traceability not being covered by SAE. IPC has good solution, IPC 1782 has been in place for 6 years but not widely adopted by industry. Distributors don't have same access to information as OEMs. That is why you need traceability.
- Blockchain hasn't been vetted yet
- We are part of Accellera Systems Initiative, use ISO/IEC 20243
- TIA SCS 9001 is a broad ICT standard, not an ME standard

Standards Recommendations (contd.)

- Company supply chain frameworks based on NIST guidance (e.g., SP 800-161)
- ISO 9001 is widely accepted across industries (e.g., AS9000/aerospace). Has elements of procurement in it
- Aerospace TORs could be “scrubbed” and made publicly available
- Develop a matrix/spreadsheet of elements in section 224 and corresponding standards
- SAE standards for counterfeit part avoidance and detection: AS6171 family of standards (testing for counterfeit and tampered parts), AS5553 (OEMs/integrators), AS6496 (authorized distributors), AS6081 (independent distributors)
- Mil PRF 38535 on performance and verification requirements of single die integrated circuit device type electronics
- NASA Solution for Enterprise-Wide Procurement (SEWP) approved contractors list https://www.sewp.nasa.gov/sewp5public/approvedcontractors and https://www.sewp.nasa.gov/documents/OTTPS-NIST_CrossWalk_NASA_SEWP.pdf
- DHS CISA's ICT SCRM Task Force has some relevant products:
- Guidance for establishing qualified bidder / approved vendor lists https://www.cisa.gov/sites/default/files/publications/ICTSCRMTF_Qualified-Bidders-Lists_508.pdf
- CISA Vendor SCRM template https://www.cisa.gov/sites/default/files/publications/ICTSCRMTF_Vendor-SCRM-Template_508.pdf
- ICT SCRM TF Report on Mitigating ICT Supply Chain Risks with Qualified Bidder and Manufacturer Lists resource https://www.cisa.gov/sites/default/files/publications/ICTSCRMTF_Qualified-Bidders-Lists_508.pdf
- Recent ITI paper on IT supply chain resiliency
- ASTM forming a new committee on supply chain

Sec 224 Vendor Demographic Considerations – Manufacturing Location

- Important if it's a contract requirement
- Does vendor provide to you vs you specifying you'll only buy from a specific location
- Design location vs final assembly and packaging location
- Do we mean only physical things (product, hardware/software)
- What visibility do we have now? How are we looking to other sectors? In food/beverage industry, yes, but not in electronics industry.
- Where is data processing happening?
- Country of origin has been the export point.
- Open source has no country of origin or is harder to identify
- Is country of origin indicated in software? Coming up in MQA
- Commercial and Government Entity (CAGE) codes morphing into company HQ.
- Guidance exists from Trade Agreements Act (TAA) (materials, products, labor). TAA is focused on majority of where manufacturing happens/where majority of costs are incurred. That is country of origin.
- Country of diffusion is where part/component was fabricated.
- There should be a hierarchy of production stages/material transformation. Country of origin should be specified at each stage
- Slave labor issue an important criteria to consider
- Geopolitical conflicts. Where is an item (noble gases) "consumed" during the production of my wafer (also applies to company ownership)

Vendor Demographic Considerations – Company Ownership

- CISA ICT SCRM vendor template
- Company can’t be on restricted/prohibited parties lists (e.g., ITAR, EAR, et al.)
- SAM/UEI has replaced DUNS/Bradford has a database in terms of use by U.S. government (USG)
- GS1 has a database that specifies organization identity all the way down to a warehouse. Hierarchical type structure. GS1 claims U.S. Customs has an initiative to turn this into a global database by end of 2022.

Vendor Demographic Considerations – Workforce Composition

- CISA ICT SCRM template has section on personnel
- Acquisition professionals could benefit from knowing questions to ask (some online training in works from group in Chantilly, VA) about letting COTS into procurement chain
- Risk related to forced (slave) labor or bad actors in the workforce who you would not want to have access to this info
- Company needs to have a sufficient vetting process that employees meet to ensure security. Not enough to just say you have to be a U.S. citizen or a lawful, permanent resident (privacy considerations come into play).
- There are export compliance requirements. That already exists. You have to fill out an I-9 form though that may not be shareable
- Has undergone training?
- NASA SEWP has best practices. Should talk to them. Embraces ISO/IEC 20243
- CFR 120.16 defines foreign persons (is broader than just U.S. citizens)

Vendor Demographic Considerations – Access to Manufacturing Data

- There are 3 buckets: 1) Have data to deliver. 2) Could generate data but don’t have it today and it comes at a cost. 3) Data we won’t share. Will you engage in the contract if the response is #3?
- Is it public or private data? Is the data readily accessible?
- Do we write into contract transition of data over to the customer?
- It should be about getting access to the data when you need it to do the analysis (not at contract point; could be end of life).
- If something goes wrong, how do I recall products affected by that malicious activity?
- Procurement often an automated process – a machine making decisions. Need to create a checklist
- What data does DoD care about? What will it hold onto? And for how long?
- How do we expect commercial entities to provide the data and how will it be accessed?
- How will vendors be “rated”?
- Using government contract flow downs may not work with COTS
- Test data packs an existing practice in the defense industry.
- COTS are without any modifications while commercial might have minor modifications about / beyond COTS
- There are contract flow downs from a company to its supplier
- Standardize the information that comes in a technical data report for COTS items.

Vendor Demographic Considerations – Reliability of Supply Chain

- Reliability of parts encoded into design automation
- Reliability means something performs as specified for a specified period of time. You expect supply chain to continue to be reliable even after parts have become obsolete. Ties in with resilience. You have to have standard practices in place to address what you know is coming.
- Counterfeiting/security issues come into play when there is no provenance. We have expectations for reliability of parts and reliability of the supply chain
- Understand this refers to supply chain of COTS provider rather than the acquirer
- What is the expiration date? Environmental conditions come into play. What happens when there are environmental changes in the distribution chain?
- Is resilience a better term than reliability? USG should define these terms.
- We want purchasing entities to behave the way we would.
- Is there integrity and security along the supply chain?
- Difference between reliability and resilience. Reliability is criteria (evaluation factors); resilience is an end state. How do we translate that into standards?

DoD Framework Approach – Compliance Suggestions (Q2b)

- Training
- Need to centralize data for less redundancy.
- Who's watching who (Dr. Seuss "bee watcher watching"). There's a whole schema associated with this. ANSI ANAB does accreditation. A2LA is another. Then there are certification bodies. Accreditation body accredits the certification body. IAB oversees country accreditation bodies. We created a standard for the accreditation bodies to do an assessment of the labs.
- PRI is the SAE performance research institute.
- 1st party, 2nd party, 3rd party certification. Think about this early on in the standards development process. What are the "shall" requirements?
- Accreditation about process; doesn't mean lab is arriving at right conclusion
- NIST just revised SP 800-161. That is the easy button.
- DHS CISA has developed a lot of guidance.
- Do I need to do V&V if I adhere to a commercial standard?
- Not everything needs outside certification; just need to prioritize
- Having a 3rd party certification/accreditation can reduce costs

DoD Framework Approach – Adoption Strategy/Timeline Suggestions (Q2e)

- There's a distinction between adoption and implementation of requirements. What needs to happen for standards to be uniformly and consistently included in a contract?
- We want to leverage what's currently happening in industry (bottom up). DOD would then tie everything up (top down). Other agencies will have their own approach.
- When SAE AS 6171 came out, there weren't any suppliers accredited to the spec
- It's important that we have broad industry and academic engagement in the development of these standards
- The standards process is slow
- Training is also important. There needs to be broad understanding among procurement officers, compliance officers, contracting officers on both the providing and receiving sides.
- ASSIST database exists once a standard/spec is adopted by DoD

Top Takeaways

- CISA ICT guide. Most of the work has already be done. People should be made aware of this.
- Ensure that solution is not overly burdensome. A significant part of the DIB already has committed to comply with the 7021 CMMC.
- Instead of viewing it as burdensome, frame it as market opportunities
- If this information was consolidated (non attributable), it might help manufacturers understand where they have monopolies/duopolies in their supply chain.
- What information? And who would benefit? OEMs. How is the information beneficial to the OEMs?
- Wear our reality hats. None of our 1000s of suppliers saw CMMC as a marketing opportunity.
- Look at GSA TIES and all companies involved in it. It’s a who’s who of the industrial base. https://www.gsaglobal.org/iot/ties/

Top Takeaways (contd.)

- There is no single overarching standard. There may be domain specific standards. We need to create the umbrella.
- Ensure Traceability and Illumination
- Leverage the good work already done (e.g., ICT SCRM TF, company best practices, etc.)
- Commerce Dept has EAR restrictions/regulations of who we do business with.
- An initiative like this needs a good communications plan in stakeholder terms. It's as much how you deliver the message than what you require. Craft the message carefully so it falls on ears of those whose cooperation we're trying to garner. Appropriate messaging leads to better adoption. Do we use "standards"? "Guidance"?
- This workshop is an important part of the messaging.
- There is a cost that companies who stay in the DIB will incur.
- How will the DoD implement its program over time to ratchet up accountability?