ANSI ME Workshop: Session 1

26 - 26 Oct 2022

Poll results

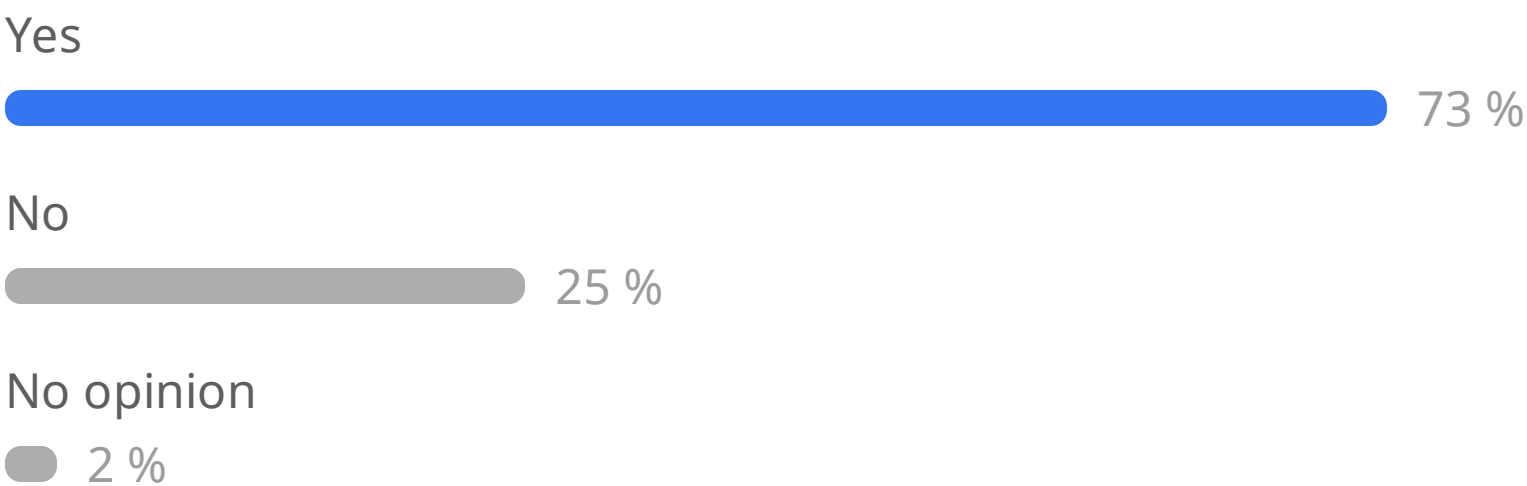
Table of contents

Multiple-choice poll

Manufacturing Locations (1/2)

0 5 2

Are these the correct considerations to define Manufacturing Location?



Manufacturing Locations (2/2)

0 3 3

Please provide any additional context around your response about the Manufacturing Location definition, such as additional emphasis on concurrences/dissents:

(1/8)

- The manufacturing location should include physical locations of all supply chain participants and constituent components for the good/service. That said, the level and depth of detail is based on the shared policy and governance models for the specific supply chain.
- I would consider manufacturing location to be the fab location, which produces the semicon die. Final test and packaging, which would yield the final product, may occur in a different location. This of course depends on one's definition of "final product".
- Given the localization of ME manufacturing to only a handful

Manufacturing Locations (2/2)

0 3 3

Please provide any additional context around your response about the Manufacturing Location definition, such as additional emphasis on concurrences/dissents:

(2/8)

of locations, only relying on a complex is woefully unrepresentative of reality. This should include materials and subcomponents not just final assembly locations. Without this centralization of assembly location there is an increase in manufacturing overhead which is difficult to compete globally. On the dev side this can be accomplished around the world, this should include how the cloud environment/dev environment is secure and where the servers physically reside.

- Would need to look at a supply/value chain map to see who/what touches the product - the provenance and pedigree.
- Traceability to raw

Manufacturing Locations (2/2)

0 3 3

Please provide any additional context around your response about the Manufacturing Location definition, such as additional emphasis on concurrences/dissents:

(3/8)

materials. Should specify that the consideration is in regards to the ME manufacturer, not higher tier integrators.

- I would disagree with government oversight of sub-tier vendors but rather task the contractor to tier down oversight to subsequent subcontractors
- The definition should define WHERE strict provenance starts. IE, can we get raw material from any country because we can test it for purity and refine it in the US, but once it starts being refined it needs to be in a friendly country etc.
- These are good considerations for defining "Manufacturing Location" but need to work on the exact content/wording.
- We need to talk

Manufacturing Locations (2/2)

0 3 3

Please provide any additional context around your response about the Manufacturing Location definition, such as additional emphasis on concurrences/dissents:

(4/8)

about specific criteria for evaluating vendors on manufacturing location. I think a lot of the discussion was more on the general approach to 224.

- other supply chain / development lifecycle--- falls in Supply Chain--- however just because it's made in USA does not make it secure/trusted
- Manufacturing location should focus on geographical location for manufacturing.
- Need supply chain info. What about in US but foreign.
- I believe that this definition aligns with the definition shared by industry. This will be important for industry adoption. I believe that we should seek to break out raw material sourcing and IP/development locations.

Manufacturing Locations (2/2)

0 3 3

Please provide any additional context around your response about the Manufacturing Location definition, such as additional emphasis on concurrences/dissents:

(5/8)

- The definition of manufacturing location should include both manufacturing activity and geo-location
- Considerations for raw material sourcing etc. would likely be included in supply chain reliability as opposed to "Manufacturing Locations"
- The last point discussing transforming into the final item seems incorrect, as packaging is that final transformative item, which is external to manufacturing. I don't think there should be a "final item" condition.
- Have to define final product
- This does not account for locations through out the microelectronics lifecycle and criticality of each phase of the lifecycle.

Manufacturing Locations (2/2)

0 3 3

Please provide any additional context around your response about the Manufacturing Location definition, such as additional emphasis on concurrences/dissents:

(6/8)

- Transformation of final item, likely misses the foundry, which Congress likely intended to be included. I would suggest the definition, but associated with specific functions (mfg, pkg, assembly, etc.)
- I would not refer to a complex, I would also consider a step in the process not related to mfg
- For consideration: level of vertical integration is what I believe was being referenced as it relates to risk.
- Agree that location of development activities should not be added into manufacturing location definition.
- You need to define location by countries in tiers, for example domestic, NTIB, NATO, UN, axis of evil, etc

Manufacturing Locations (2/2)

0 3 3

Please provide any additional context around your response about the Manufacturing Location definition, such as additional emphasis on concurrences/dissents:

(7/8)

- Manufacturing location also would include upstream fab locations or sub manufacturing locations, the manufactruing location is the last location before shipping
- Do need more clarity on development and fab
- "...which transforms into the final item" missing the what.
- Details should be in supply chain. This is focusing on country laws and politics
- There needs to be considerations for exactly what “process which transforms into the final item” means. How far back does this go?
- In part but we need to clarify how deep we need to go into supply chain
- This definition of

Manufacturing Locations (2/2)

0 3 3

Please provide any additional context around your response about the Manufacturing Location definition, such as additional emphasis on concurrences/dissents:

(8/8)

"location" focuses on the physical structures, and omits the geographic location of those structures

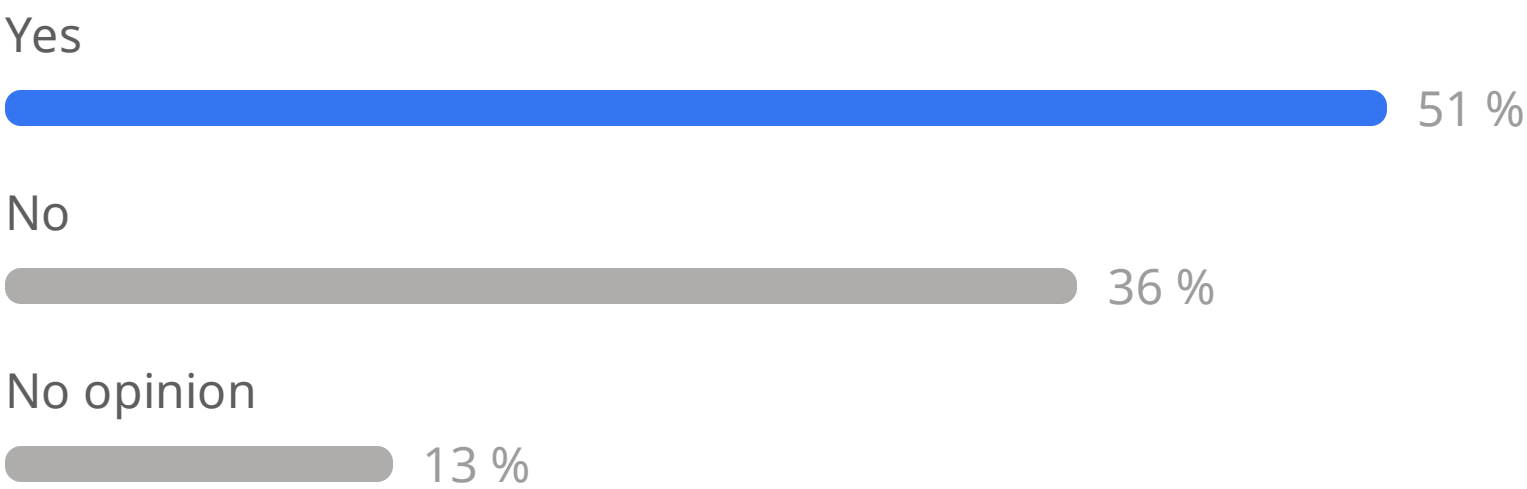
- This should be part of the risk mitigation considerations - so alternate locations, etc would be part of the requirements to determine risk
- What happens when manufactring moves from friendly to non-friendly countries
- It is where the final product is sourced from

Multiple-choice poll

Company Ownership (1/2)

0 3 9

Are these the correct considerations to define Company Ownership?



Company Ownership (2/2)

028

Please provide any additional context around your response about the Company Ownership definition, such as additional emphasis on concurrences/dissents:

(1/7)

- Very complex due to different country regulations. How much influence does HQ have across various locations. Ex. HQ in US with operation in China will be influenced more by local regulations versus HQ direction.
- Self attestation would be required here since company ownership may not be fully verifiable.
- The definition seems appropriate.
- The question is whether the ownership definition and supporting evidence may be trusted. Is this self-endorsed or third-party endorsed? The policy and governance structure will help define this.
- Agree with comments made about layers of complexity with defining true ownership

Company Ownership (2/2)

0 2 8

Please provide any additional context around your response about the Company Ownership definition, such as additional emphasis on concurrences/dissents:

(2/7)

given VCs, etc. I do also agree with comments made about recreating the wheel and are we coming up with redundant definitions to what already exists? I.e. in relation to SEC, DFAR references.

- Foreign influence should also be evaluated. Influence is not necessarily coupled to ownership.
- I like all the words there- but do not think DoD should work this indep of DOS etc... next paragraph that says leverage FOCIS, CFIUS etc... is a better start point... also agree SEC definitions may already have def/info on publicly traded companies...
- Leverage existing definitions in requirements/language in other regulations.
- Recognition of how

Company Ownership (2/2)

0 2 8

Please provide any additional context around your response about the Company Ownership definition, such as additional emphasis on concurrences/dissents:

(3/7)

dynamic this issue is with constant mergers, acquisitions, etc.

- I believe we should limit the scope of discussion to DSS definitions and leverage policies and procedures already in place
- Can’t possibly repeat all the considerations that have been discussed
- Expand to include market factors, any applicable regulatory and legal definitions
- I support the idea of using DFARS and DSS sources of information in this criteria
- But probably additional risks other than purely ownership (e.g., other forms of influence)
- If applying zero trust properly (ie, a truly asset- and data-centric approach), does nationality

Company Ownership (2/2)

0 2 8

Please provide any additional context around your response about the Company Ownership definition, such as additional emphasis on concurrences/dissents:

(4/7)

of employees matter as long as correct controls are in place to address it?

- Access to Public vs Private needs to be considered. Also appreciated the comment on resources available to assist with the calculations, etc.
- it's a good starting point to defining considerations
- It's a reasonable place to start with the discussion.
- Blue definition 2nd and 3rd bullet
- should be expanded to include current govt regulations such as DFARS, FARs, DSS
- Emphasis on cfius, firrma, and the recent executive order strengthening cfius considerations
- Location/foreign conversations need to be

Company Ownership (2/2)

0 2 8

Please provide any additional context around your response about the Company Ownership definition, such as additional emphasis on concurrences/dissents:

(5/7)

considered within the definition

- Definition works for workshop, but needs nuance in the long term. The discussion identified some excellent additions here - influence vs. ownership, opaqueness of ownership, public vs. private, etc.
- Issues of how ownership/influence is determined especially for smaller companies
- There has to be a standard way to identify company lineage and what country laws they are required to follow in order to conduct business. This is a procurement issue and not just a manufacturing requirement.
- For the most part it is correct, but I would focus more

Company Ownership (2/2)

0 2 8

Please provide any additional context around your response about the Company Ownership definition, such as additional emphasis on concurrences/dissents:

(6/7)

on influence rather than ownership. Major customers could have significant influence over a Company. [redacted] is a prime example of a company that is heavily influenced by their revenue ties to China.

- I understand this will not be easy but there should be a specific percentage threshold to determine ownership and control. Or at least flexibility to examine on a case-by-case basis. Should focus not just on whether vendor is based in US but also other "trusted" countries (TAA countries is a good place to start).
- major company relations should also be included.
- I think we have to

Company Ownership (2/2)

0 2 8

Please provide any additional context around your response about the Company Ownership definition, such as additional emphasis on concurrences/dissents:

(7/7)

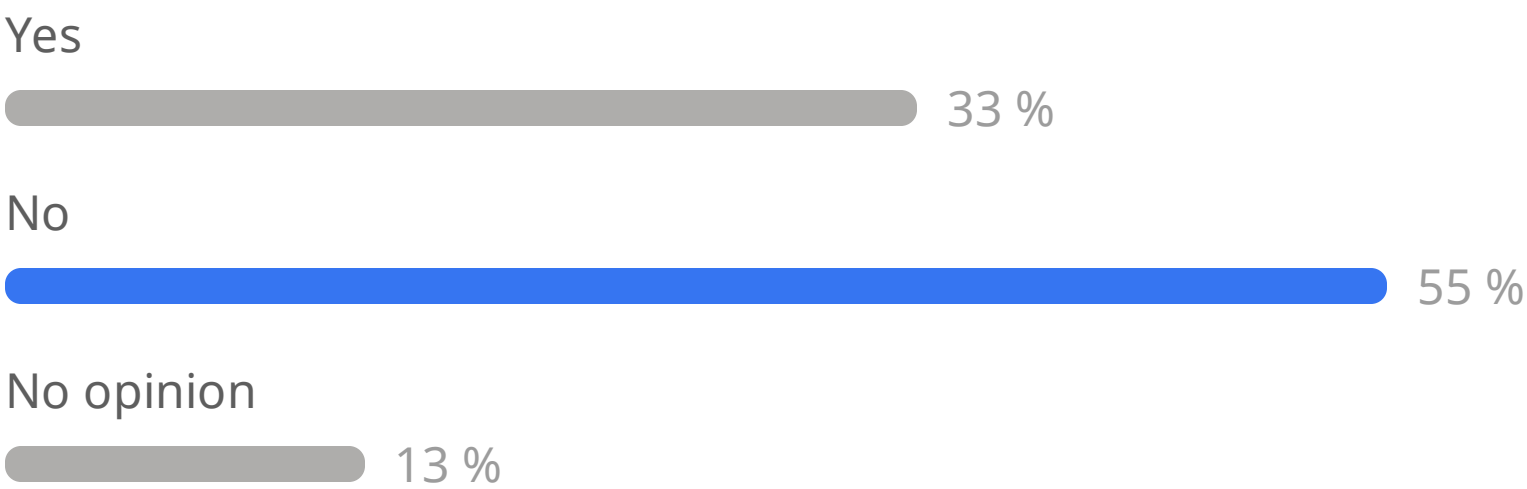
really think about how this factors into the risk for COMMERCIAL companies.

Multiple-choice poll

Workforce Composition (1/2)

0 4 0

Are these the correct considerations to define Workforce Composition?



Workforce Composition (2/2)

0 3 5

Please provide any additional context around your response about the Workforce Composition definition, such as additional emphasis on concurrences/dissents:

(1/13)

- Strike “age” from list of considerations and only apply nationality requirements to products with highest levels of criticality
- I think you need both 1&2 I think the three major categories of concern (not education, citizenship, age): (1) Skillset Qualification (education, certification, experience) (2) Allegiance (to US to others / may be tied to US Citizen/ person v. foreign citizen (3) Moral violation- child labor / forced labor linking

Workforce Composition (2/2)

035

Please provide any additional context around your response about the Workforce Composition definition, such as additional emphasis on concurrences/dissents:

(2/13)

to notional LOAs A- is cleared personnel (Govt clearance) B- US Citizen / US person &/or some sort of background check by employer C- other D- individual restrictions... or categories

- From a workforce perspective, allegiances of members of the workforce seems important. Not sure how one gets at that...maybe some sort of clearance process. Still the results are not devoid of risk.
- consider privacy issues; standardized training
- Frequency of vetting/screening should also be a factor as these things are subject to change (e.g. citizenship/allegiance, criminal behavior).
- This should be %'s or

Workforce Composition (2/2)

035

Please provide any additional context around your response about the Workforce Composition definition, such as additional emphasis on concurrences/dissents:

(3/13)

other generic data. Details open significant legal jeopardy / liabilities to the company.

- Focus should be on trustworthiness
- I agree with the summary of items to evaluate: Loyalty, Qualifications, Moral. However, I think Moral is covered under other procurement requirements (slavery and human trafficking prevention) and Qualification for production quality would be addressed with something like iso9001 requirements. Maybe

Workforce Composition (2/2)

0 3 5

Please provide any additional context around your response about the Workforce Composition definition, such as additional emphasis on concurrences/dissents:

(4/13)

assess security training for workforce? Loyalty is a big one for this, but might be legally difficult to assess and require beyond a citizenship requirement.

- Challenging to implement. Particularly outside of US.
- Focus should be I'm on skill/training of worker rather than demographics, but citizenship is still an important criteria as it pertains to worker allegiance. Agree this should be self attested and not submitted info
- it is not only access to IP, but physical access to manufacturing location areas that can impact production
- This should follow western

Workforce Composition (2/2)

035

Please provide any additional context around your response about the Workforce Composition definition, such as additional emphasis on concurrences/dissents:

(5/13)

norms along with US laws and GDPR. Should not bend to chinese considerations. Employees shall be allowed to freely pursue employment opportunities, this includes the freedom to quit if they do not like the work environment. Employees shall be free to move to any region within
the country to work to pursue better opportunities. Best practice is that employees are not held to non-compete agreements, this is one of the reasons for Silicon Valley's success. Another best practice is tracking which employees have touched manufacturing and development for each part of a widget.

- How will companies protect trade

Workforce Composition (2/2)

035

Please provide any additional context around your response about the Workforce Composition definition, such as additional emphasis on concurrences/dissents:

(6/13)

secrets from employees departing abroad?

- I would expand the 'Training' items around workforce pipeline, apprenticeships. and [redacted] categories: ○ Qualifications ○ Allegiances Mores
- The first bullet seems OK, but the second bullet does not make sense. It needs to be rewritten.
- Should reflect critical skill set, proficiency in skill set, and redundancy of critical skills , not specific age
- Enforcement and consistency of evaluation are going to be really hard in this category beyond citizenship / residency. We haven't heard from industry about increases to hiring costs, legal peril, etc. for secure microelectronics

Workforce Composition (2/2)

035

Please provide any additional context around your response about the Workforce Composition definition, such as additional emphasis on concurrences/dissents:

(7/13)

- This is problematic as lower levels supply chain personnel will not want details of their staff being exposed at higher levels in the hierarchy. This will become too big at the top of teh supply chain hierarchy and will become a high target for malicious attacks. Therefore suppliers needs to gather
this info and keep it secured within their companies and only provide access to it via a controll access and only to those who are have clearance to see that type of data. I only want my supplier to validate taht they have done the background checks of their employees.
- There needs to be considerations for distinguishing between those employees directly involved with

Workforce Composition (2/2)

035

Please provide any additional context around your response about the Workforce Composition definition, such as additional emphasis on concurrences/dissents:

(8/13)

manufacturing the MEs as compared to the entire workforce of the organization.

- I'm unsure on the legal practicality or utility of applying this definition. I doubt the commercial industry will embrace or disclose these data due to privacy. This seems like a requirement to be defined in a purchase request (e.g., staffed by screened persons by the European Criminal Records Information Services) rather than a policy stance.
- Regarding workers in the EU; It might be worthwhile to find out how [redacted] and other companies in the EU are currently vetting their workers.

Workforce Composition (2/2)

035

Please provide any additional context around your response about the Workforce Composition definition, such as additional emphasis on concurrences/dissents:

(9/13)

- Seems like workforce composition is tied to ownership and key management also. Much of this seems more like a suggested best practice - like training. And a company might have thousands of employees - how does this apply (to all, to a few that are known to be directly involved in the mfg process?)
- I don't need to know the details about individual people. But the company should be able to make an assertion with the potential for an audit.
- Should consider local law when conducting background checks. We should require US oversight of foreign nationals. Which has been agreed to in the past as part of the risk mitigation approach.
- Things beyond the

Workforce Composition (2/2)

035

Please provide any additional context around your response about the Workforce Composition definition, such as additional emphasis on concurrences/dissents:

(10/13)

scope of security should not be a consideration e.g., ethics considerations like child labor. Workforce composition should be based more about political threats for IP theft/malicious attacks and therefore more geographically-based and evaluated based on export control tiering.

- overkill. The contractor shall have the latitude to select employees provided that they meet the requirements of the contract including the delivered product meets all performance, QA and labor and environmental laws
- Criteria should include what they do about issues in demographics,

Workforce Composition (2/2)

035

Please provide any additional context around your response about the Workforce Composition definition, such as additional emphasis on concurrences/dissents:

(11/13)

for example knowledge management and transfer for aging workforce

- Need to consider local laws, minimum age varies, how do we manage these?
- How do these attributes impact secure ME? Ability and education may have more to do with how good a product is not how secure
- Agree with comments

around skill set focus and companies having the right process in place to ensure they are addressing workforce concerns. While demographics are important to ensure companies are following the law in their respective countries, it isn't the only focal point.

- Need to add # of employees, years

Workforce Composition (2/2)

0 3 5

Please provide any additional context around your response about the Workforce Composition definition, such as additional emphasis on concurrences/dissents:

(12/13)

of experience based on age of employees. Doesn't help if 95% of the work force is under 30 with no experience as well as the opposite, Disney help if 95% of the work force has 30 years of experience andwill be gone in a few years

- Metric for Turnover (i.e. how long have personnel filling critical positions worked for the company?) Metric for Knowledge Management
- I think that this needs to be more process oriented based upon the objectives of securing ME supply chain. We need to focus on defining those criteria.
- How is this different from racial profiling.
- I would remove age and

Workforce Composition (2/2)

0 3 5

Please provide any additional context around your response about the Workforce Composition definition, such as additional emphasis on concurrences/dissents:

(13/13)

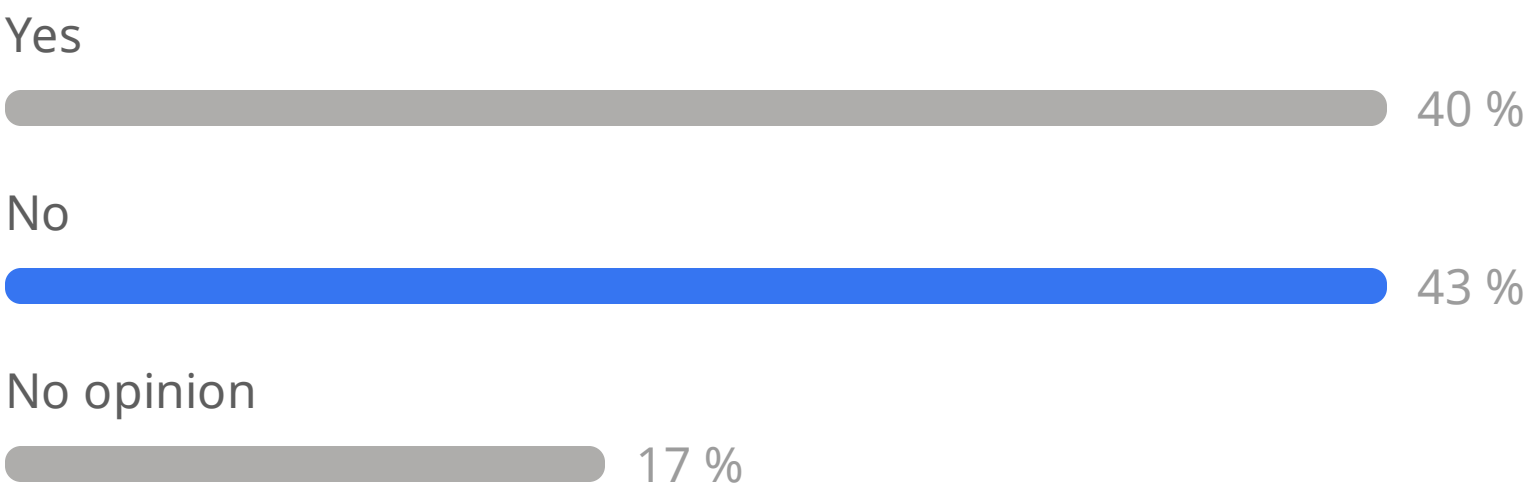
education as I am unsure that there is a reliable data source for this information

Multiple-choice poll

Access to Manufacturing Data (1/2)

0 3 5

Are these the correct considerations to define Access to Manufacturing Data?



Access to Manufacturing Data (2/2)

0 2 8

Please provide any additional context around your response about the Access to Manufacturing Data definition, such as additional emphasis on concurrences/dissents: (1/10)

- Per the CUI discussion, the controls that allow the companies to handle CUI may be a valuable LOA A or B guideline even though COTS is not subject to them.
- The difference between authorized access (e.g., up through the supply chain) vs. unauthorized access (e.g., with malicious intent or inadvertent) Some audits are necessary and are a cost of doing business so don't rule them out. Paying for an audit can sometimes be cheaper if it limits the amount of audits and access. Sending someone an acceptable cert in many cases stops a lot of questions.
- Access Controls should at a minimum

Access to Manufacturing Data (2/2)

0 2 8

Please provide any additional context around your response about the Access to Manufacturing Data definition, such as additional emphasis on concurrences/dissents: (2/10)

pass an audit by externally certified organization preferably one of the big four, such as [redacted]

- Should focus on physical security. But why is this a consideration for COTS
- We need to address the full lifecycle for producing ME; we also don't need to reinvent all these terms and concepts and should use industry recognized cert. programs that already address this.
- Additional consideration toward customer information protection. Not just IP but purchasing entities and chain of custody.
- Physical security and cyber security would need to be represented

Access to Manufacturing Data (2/2)

028

Please provide any additional context around your response about the Access to Manufacturing Data definition, such as additional emphasis on concurrences/dissents: (3/10)

in criteria related to the access during manufacturing consideration.

- Don’t reinvent the wheel here. For non-commercial products, including NDI, the government has substantial access to contractors, their subcontractors and sub-tier vendors thru FAR QA and higher-level QA Mgmt Systems (ISO 9001, AS9100, etc.) requirements. Access to commercial product (aka COTS) manufacturers is what we should be focusing on and in my opinion, I

Access to Manufacturing Data (2/2)

0 2 8

Please provide any additional context around your response about the Access to Manufacturing Data definition, such as additional emphasis on concurrences/dissents: (4/10)

am steering me to ISI/IEC 20243, which is not DoD adopted. FYI, for COTS data we already impose requirements for the sources of electrical and electronic thru the DFARS 25.246-7008(?)

- The big challenge here is to identify what information needs to be provided in order to quantitatively measure trust.

It is important to make sure the data generated is generated and collected within the existing manufacturing framework.

- Access has to be examined in the context of who needs to know/have access. Just a blanket statement like "What access to 'you' have . . ." doesn't address the issue appropriately
- YES- agree all, but... If

Access to Manufacturing Data (2/2)

028

Please provide any additional context around your response about the Access to Manufacturing Data definition, such as additional emphasis on concurrences/dissents: (5/10)

just Confidentiality--- leverage NIST 800-171 & DoD CMMC (may be too network specific) Why limited to MFG --- should really be pursuing "limited role base access" throughout the lifecycle.. if COTS--- may not involve CUI & CMMC... but could have some sort of "commercial standard" on role-based access

- I think there was a lot of good discussion around this that words in this criteria are unclear of who the "you" is and who we are taking about accessing things.
- Maturity of the companies' policies; COTS development look at applicability of ISO/IEC/IEEE standards on supply chain of this topic for COTS
- Business related infrastructure should be isolated from

Access to Manufacturing Data (2/2)

028

Please provide any additional context around your response about the Access to Manufacturing Data definition, such as additional emphasis on concurrences/dissents: (6/10)

manufacturing infrastructure (SCADA). This is really a security best practice, but may need to be emphasized for any assurance standard.

- This is not focusing on commercial products. This is too much focused on DOD products and assumptions.
- First the Manufacturing scope should be expanded to all the steps in teh Product life Cycle - Every step should be role based access control and not just manufacturing. Physical access to the manufacturing site is critical and without that

Access to Manufacturing Data (2/2)

028

Please provide any additional context around your response about the Access to Manufacturing Data definition, such as additional emphasis on concurrences/dissents: (7/10)

it is an immediate dis-qualifier. Role based acess control is minimum criteria for all criteria associated with all 4 combinations of Material and/or Information - Transfer and /or modification.

- Lifecycle data should be provided based on the policy and governance requirements.

Recommend IETF SCITT for management of these lifecycle artifacts: https://github.com/ietf-scitt/use-cases/blob/main/hardware_microelectronics.md

- I prefer the definition that goes back to role-based access to data and physical elements. Enforcement (leveraging existing audits, auditability,

Access to Manufacturing Data (2/2)

028

Please provide any additional context around your response about the Access to Manufacturing Data definition, such as additional emphasis on concurrences/dissents: (8/10)

etc.) all come into play. I'm also worried that we're writing criteria appropriate to custom devices vs. COTS

- Rather than access to have to alter or sabotage, change it to access to violate the integrity of operations.
- Need to understand the amount of foreign national or potential personnel that might be a factor.
- Yes, but this one needs so much more
- Maturity of these needs to be done through audit, perhaps there exists audits we can leverage.
- We really need to think of this in terms of risk management. While these questions are centered around the right

Access to Manufacturing Data (2/2)

028

Please provide any additional context around your response about the Access to Manufacturing Data definition, such as additional emphasis on concurrences/dissents: (9/10)

areas the conformance requirements are the objective. Each company will have a different approach based on their different manufacturing processes. These requirements were laid out in ISO/IEC 20243 in
the previous work that was done by DoD under CNCI. Suggest we use that

as top cover and bring some of the more detailed standards and testing underneath.

- Covered under NIST 800-171. Cyber CIA should apply. Minimum criteria should be physical and internet access controls in place with potential audits.
- Company making commercial products must have access to the

Access to Manufacturing Data (2/2)

0 2 8

Please provide any additional context around your response about the Access to Manufacturing Data definition, such as additional emphasis on concurrences/dissents: (10/10)

IP they need for the product. Maybe the question is how does the company know that they have used IP that is clear of weaknesses.

- This needs to also answer the question: what secondary geo-political risks are there for third party vendors/countries?
- I would add Cyberseurity risk posture (we utilizing Security Scorecard)
- The NIST SP 800-171 covers most of this and is already a requirement throughout the DIB.

Multiple-choice poll

Reliability of the Supply Chain (1/2)

0 3 4

Are these the correct considerations to define Reliability of the Supply Chain?

Reliability of the Supply Chain (2/2)

0 2 5

Please provide any additional context around your response about the Reliability of the Supply Chain definition, such as additional emphasis on concurrences/dissents:

(1/9)

- What are the controls to ensure the compliance of the supply chain?
- On the logistical side, national allegiance. For example, if a manufacture establishes a fab in China and in Russia, is that effective for availability. Alternatively, shouldn't companies be able to manage this based on the going concern principle, but when countries are subsidizing specific critical areas, maybe government should be increasing import taxes on these specific

Reliability of the Supply Chain (2/2)

0 2 5

Please provide any additional context around your response about the Reliability of the Supply Chain definition, such as additional emphasis on concurrences/dissents:

(2/9)

items to level the playing field. Integrity and confidentially levels, there needs to be a coordination between US and other law enforcement agencies such as Europol etc to hold malicious actors in line.

- It's not just about consistency. It's about meeting a stated set of requirements and expectations, just as reliability is defined for any application. Resilience should be included in connection with the bullet about "Should include interferences . . . " - it is about resilience to those factors. Contracting Considerations is too ambiguous. How do we know what that even means? Reliability of the supply chain is the top level issue - it should not be repeated as an element of the definition

Reliability of the Supply Chain (2/2)

025

Please provide any additional context around your response about the Reliability of the Supply Chain definition, such as additional emphasis on concurrences/dissents:

(3/9)

- with qualification as this requirement overlaps with the OSD SCRM WG. With regard to discussion of COTS SCR, I defer once again to the ISO/IEC 20243 documents
- In my opinion, this is the top level consideration. All the other considerations roll up into Reliability of the Supply Chain.
- May need to start with what the definition of what reliability is.
- Yes, but I did like the comment about interweaving elements from NIST 161, etc. Also agree with and would extend on Dan's comments re: this making more sense in the context of a ven diagram than individually. (but this the necessary precursor)
- We need to include aspects of political unrest as well

Reliability of the Supply Chain (2/2)

025

Please provide any additional context around your response about the Reliability of the Supply Chain definition, such as additional emphasis on concurrences/dissents:

(4/9)

as natural disasters as it relates to sustained reliability.

- Access to supply should be considered in light of total demand from all customers
- material shortages and components: Conflict material, RoHS requirements present in COTS vs. boutique parts.
- Trying to maintain a narrow focus here.... I see Reliability as the combination of resilience and recovery. Some of the extra bullets, Counterfeit for example, don't belong here. I think they are better suited in a section that addresses assurance. Reliability should be addressed as it relates to securing the ME supply chain and not just reliability per se.
- Yes these points are valid but

Reliability of the Supply Chain (2/2)

0 2 5

Please provide any additional context around your response about the Reliability of the Supply Chain definition, such as additional emphasis on concurrences/dissents:

(5/9)

they are not adequate for completeness. A seperate bullet is reuired for the loading and consumption of data into software tools to reduce the human entry errors that contribute to 24% of wasted engineering resources that are spent
fixing these errors. Reliability of the Supply Chain is perceived as availability of parts wherein it should be about security, trust and availability of the parts in teh supply chain, against malicious actions, counterfeits, and manufacturing process deficiencies.

- The evaluation based on the criteria established should reflect an end state level of resilience

Reliability of the Supply Chain (2/2)

0 2 5

Please provide any additional context around your response about the Reliability of the Supply Chain definition, such as additional emphasis on concurrences/dissents:

(6/9)

i.e., how well a program can adjust based on the realization of supply chain risks

- The bulk of this content classic logistics SCRM (maybe ISO 9000 quality & classic Availability)... NEED to also address CUI concerns in HwA & SwA... adding Cyber-SCRM construct like NIST 800-161 & applicable commercial standards like ISO 20243, etc... can't exclude COTS from notional LOA A or B... DD
- Seems more like a system level consideration than one of commercial microelectronics. Unless we are also considering the end use factors

Reliability of the Supply Chain (2/2)

025

Please provide any additional context around your response about the Reliability of the Supply Chain definition, such as additional emphasis on concurrences/dissents:

(7/9)

that involve use of COTS in gov't and critical infrastructures and those supply chain reliabilities (vs cots chip fab supply chain?)

- Include mapping of supply chain. Some risks might be mitigated by assessing supporting circuitry vs critical parts. When can you buy/use stored parts.
- Should include process controls. Also might there be a difference in risk related to reliability of the supply chain for steady state supply chain operations and supply chain operations under stress (e.g., conflict, pandemic, other natural disasters)?
- Need consideration toward internal controls/processes for production support: volume of production, planning organization, QMS systems, etc

Reliability of the Supply Chain (2/2)

025

Please provide any additional context around your response about the Reliability of the Supply Chain definition, such as additional emphasis on concurrences/dissents:

(8/9)

- I really think we need to look at this from the perspective of trust There are lots of commercial applications that require at least some degree of trust, ie autonomous vehicles, banking and telecommunications
- the term "performance" is the focus of the defintion but not defined. Interpretation of the definition by itself does not align with the other bullet points. Suggest to state "performance, output and availability" instead in the definition
- Consider "resilience" in place of (or at least in addition to) reliability
- Reliability and resilience require end-to-end visibility, lead time,

Reliability of the Supply Chain (2/2)

0 2 5

Please provide any additional context around your response about the Reliability of the Supply Chain definition, such as additional emphasis on concurrences/dissents:

(9/9)

supplier diversification, data/digital twins, and sustainable practices.

- I would caution against including factors that are outside of a supplier's control. Perhaps items such as redundancies in that LoA-A Category but including it as a minimum acceptable criterion could eliminate several smaller and essential suppliers.
- There are other standards in place from NIST and SAE that address it.
- This is a good starting list. Somehow we also need to capture lead times and I'm not sure if it's here or elsewhere for procurement considerations.