ANSI / DoD Microelectronics Standards Workshop

Workshop Objectives

Christine Rink
OUSD(R&E) / CT , Microelectronics

ANSI Workshop
26 Oct 2022

Motivation: FY20 NDAA Section 224
Trusted Supply Chain and Operational Security Standards

1) b) Standards Required
   - *A. Not later than January 1, 2021, the Secretary shall establish trusted supply chain and operational security standards for the purchase of microelectronics products and services by the Department.*
   - *B. For purposes of this section, a trusted supply chain and operational security standard—*
     - i. is a standard that systematizes best practices relevant to—
       - I. manufacturing location;
       - II. company ownership;
       - III. workforce composition;
       - IV. access to manufacturing data;
       - V. reliability of the supply chain; and
       - VI. other matters germane to supply chain and operational security; and
     - ii. is not a military standard …

4) The standards established … shall be, to the greatest extent practicable, generally applicable to the trusted supply chain and operational security needs and use cases of the United States Government and commercial industry, such that the standards could be widely adopted by government agencies, commercial industry, and allies and partners of the United States as the basis for procuring microelectronics products and services.

Standards should include congressionally specified information and address needs of commercial industry

Definitions

Commercial

A product, that is of a type customarily used by the general public or by nongovernmental entities for purposes other than governmental purposes, and has been sold, leased or licensed or offered for sale, lease or license to the general public

A product that would satisfy a criterion expressed in paragraph (1) or (2) of this definition, except for-

- Modifications of a type customarily available in the commercial marketplace; or
- Minor modifications of a type not customarily available in the commercial marketplace made to meet Federal Government requirements. "Minor modifications" means modifications that do not significantly alter the nongovernmental function or essential physical characteristics of an item or component, or change the purpose of a process. …

FAR 2.101 (summarized)

COTS

Commercial off the Shelf

1. Is a commercial product
2. Sold in substantial quantities in the commercial marketplace; and
3. Offered to Government without modification

COTS are a subset of commercial products

FAR 12.505 (summarized)

Hardware Assurance

An activity to ensure a level of confidence that microelectronics (also known as microcircuits, semiconductors, and integrated circuits, including its embedded software and/or intellectual property) function as intended and are free of known vulnerabilities, either intentionally or unintentionally designed or inserted as part of the system's hardware and/or its embedded software and/or intellectual property, throughout the life cycle.

DAU Glossary

Workshop Objectives

OBJECTIVE #1

Identify the appropriate set of considerations for each supply chain practice area

OBJECTIVE #2

Develop baseline criteria for secure microelectronics to be used in DoD systems and national critical infrastructure

OBJECTIVE #3

Identify appropriate references

OBJECTIVE #1: Identify Considerations

Each supply chain area (breakout) will receive candidate considerations

- Considerations were informed by ANSI Workshop #1 proceedings
- Definitions language leverages publicly available standards (e.g., NIST) when possible, or is identified as a strawman
- Should be broadly applicable, and not specific to DoD

Breakouts should evaluate and improve candidate considerations

- Is the list complete?
- Are all items appropriate?
- Are all necessary terms crisply defined?

Breakout should identify and define considerations for their supply chain practice area

OBJECTIVE #1: Identify Considerations

Baseline Assumption – Do Not Reinvent the Wheel

- Some supply chain practice areas have significant overlap with existing standards (e.g., Procurement Management, Information & IP Protection)
- Sec 224 activities should seek to leverage existing efforts and add value by
  - Specifically addressing considerations that address Sec 224 and/or assured microelectronics and/or
  - Informing DoD's response to Congress (e.g., what is untenable, missing, etc.?)

Workshop only: assume application of NIST SP 800-161r1 as notional baseline

- NIST publications are available free of charge and can be accessed by all workshop participants
- NIST SP 800-161 has already been evaluated and mapped by other USG entities
- Relevant links
  - NIST SP 800-161 Rev. 1: Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations
  - NASA SEWP Standards Crosswalk: ISO 20243 & NIST 800-161
  - DHS CISA ICT SCRM Task Force: CISA Vendor SCRM template
  - DHS CISA ICT SCRM Task Force: ICT SCRM TF Report on Mitigating ICT Supply Chain Risks with Qualified Bidder and Manufacturer Lists

OBJECTIVE #2: Develop Criteria

Industry has repeatedly advocated for a scoreboard that helps them to understand and service a market for secure microelectronics

Breakouts should work to develop criteria to support Levels of Assurance

- Preferred workshop output is identifying baseline criteria to be considered secure microelectronics that can be used in DoD and national critical infrastructure systems
  - In some cases it may be easier to develop criteria for the highest level of assurance and what is considered unacceptable for use in those systems
- Leverage existing value judgements when practicable (don't reinvent the wheel)
- Teams may choose a single criteria statement or develop a statement for each area of consideration identified for objective #1

OBJECTIVE #2: Develop Criteria

Candidate LoA descriptions for use in this workshop focus on:

- Is the resultant device considered secure microelectronics or not?
- Is additional risk management needed for use in DoD or national critical infrastructure? (no need to define what those mitigations are yet)

Preferred outcome: LoA B criteria defined

LoA: A	Devices that meet or exceed these criteria are considered secure microelectronics and are appropriate for use in DoD or national critical infrastructure systems. Criteria represent a preferred or best-in-class microelectronics security solution. (e.g., highest level of assurance)
LoA: B	Devices that meet these criteria are considered secure microelectronics and may be appropriate for use in DoD or national critical infrastructure systems. Additional risk management may be necessary if used for critical functions. (e.g., baseline level of assurance for national critical infrastructure)
LoA: C	Devices in this category are not considered secure microelectronics. Programs should actively manage the risk associated with these devices if they are used in national critical infrastructure.
LoA: D	Devices in this category are not considered secure microelectronics, and represent a risk to DoD systems. Devices should not be used in DoD systems or national critical infrastructure in the absence of a technically rigorous waiver process that includes decision making at a higher level than the program.

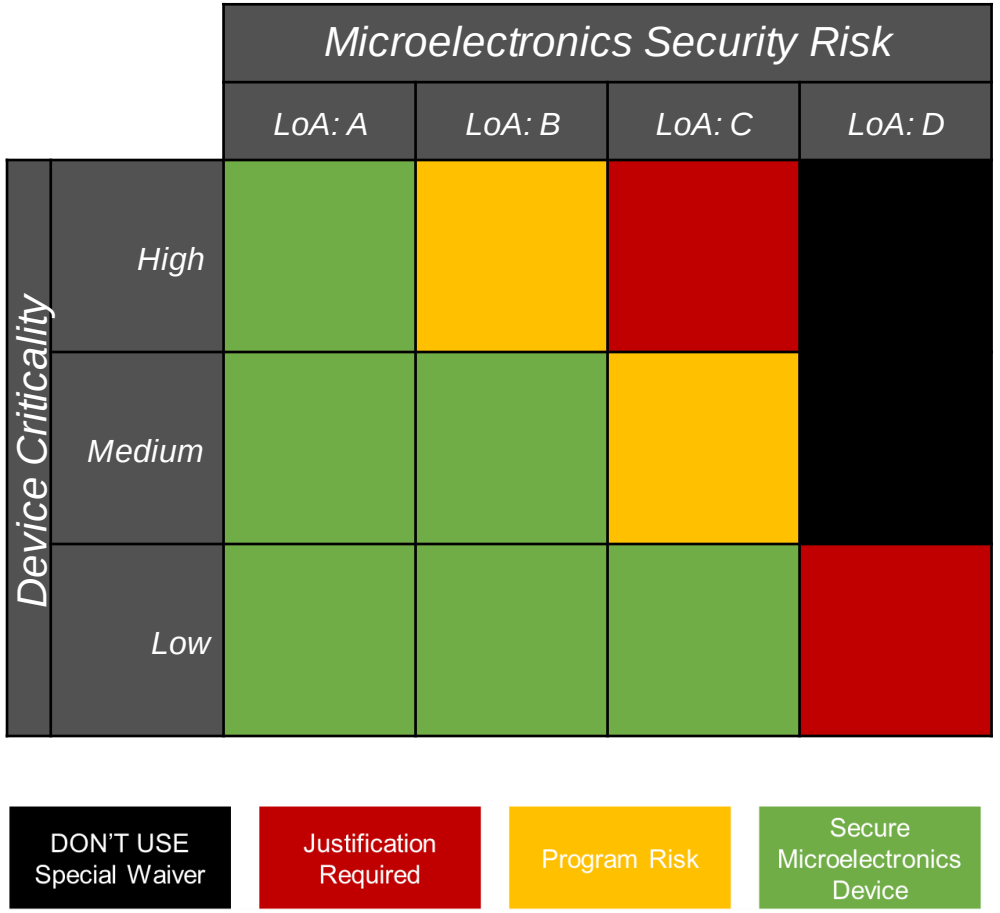
OBJECTIVE #2: Develop Criteria

Graphic provides notional example of how LoAs may be used by programs or system integrators

- Application of the LoAs is beyond the scope of this workshop, but a notional graphic is shown

Objective #2 focuses on defining LoA criteria

- Preferred: LoA B
- Alternative: LoA A *and* (LoA D *or* LoA C)



OBJECTIVE #3: Identify Appropriate Resources

Each supply chain area (breakout) will receive a starter list of references

- Informed by ANSI Workshop #1
- Broken into four categories of resources:
  - Regulation
  - Policy
  - Standards and Best Practices
  - Other

Breakouts should add references

- Limit time spent (i.e., 15-30 minutes), as this is not a primary objective

BACKUP

Slides from ANSI Workshop #1

Microelectronics Standards – Section 224

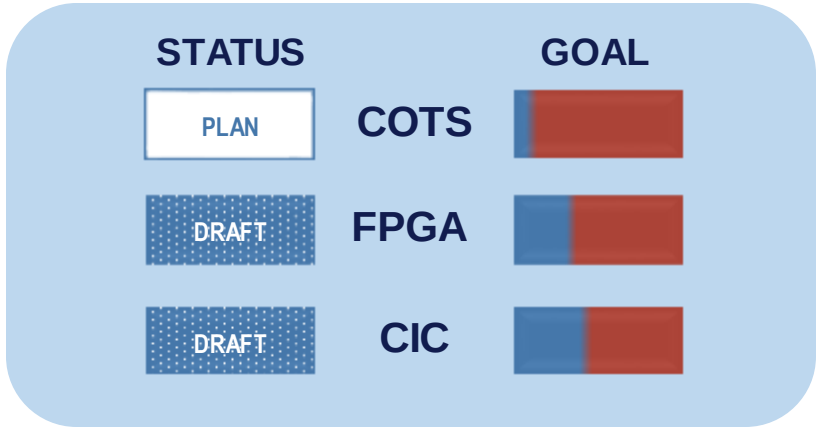
Legend	
BLUE	R&E/CT Deliverable
RED	Commercial Document
GREEN	Other DoD Documentation

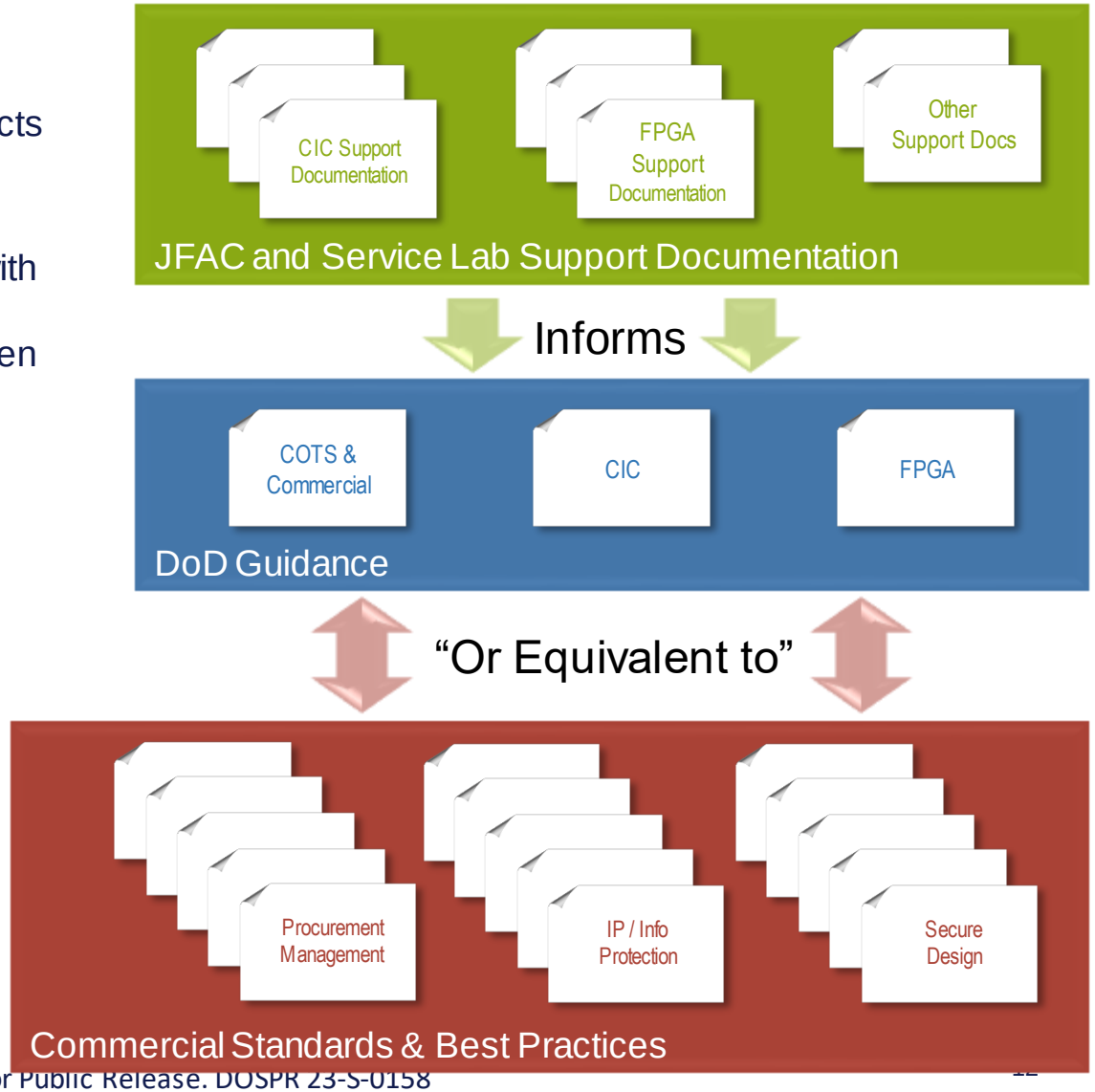
DRIVER

- FY20 NDAA Sec 224 – "… shall establish trusted supply chain and operational security standards for the purchase of microelectronics products and services by the Department"

PLAN

- ANSI engagement to evaluate and populate DoD assurance framework with commercial standards across multiple categories
- DoD standards guidance identifies requirements to close any gaps between commercial standards and DoD assurance requirements
- Leverages commercial standards to the extent practicable
- Annual updates





CIC	Custom Integrated Circuit
COTS	Commercial Off The Shelf
FPGA	Field Programmable Gate Array

Approach: Risks, Vulnerabilities, Threats

The microelectronics standards approach utilizes CIA triad

- Commonly used in networking / information security

Confidentiality (C)
Preserving authorized restrictions on information and/or intellectual property access and disclosure

1) **Theft of Design**
2) **Theft of Device**
3) **Theft of Runtime Data**

Loss of confidentiality results in the unauthorized disclosure of information and/or intellectual property, to include the physical element

Integrity (I)
Guarding against malicious information/intellectual property addition, modification, and/or deletion and ensures authenticity

1) **Modification of Design**
2) **Modification of Device**
3) **Modification of Runtime Data**

Loss of integrity results in the unauthorized addition, modification, or removal of information, IP, or physical element

Availability (A)
Ensuring timely and reliable access to and use of suppliers and sources

1) **Accessibility of Sources**

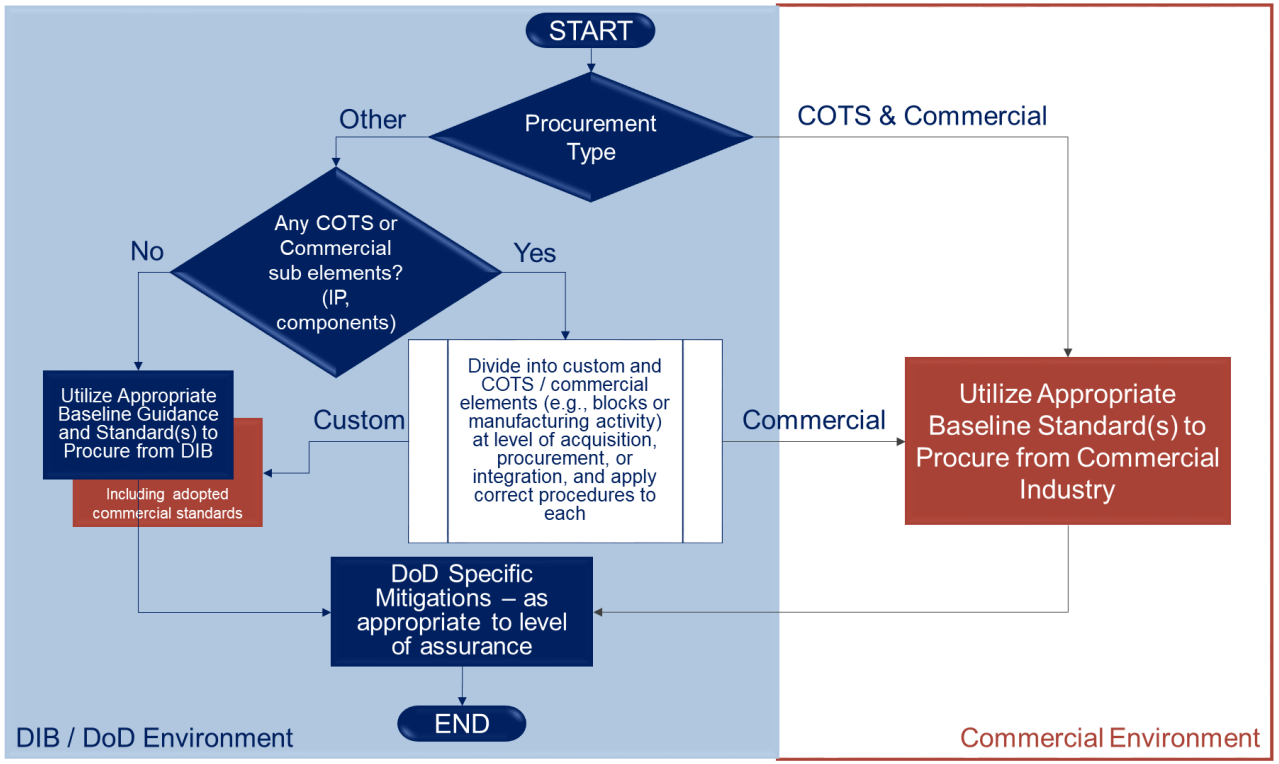
Loss of availability results in the disruption of access to or use of products or services necessary to the supply chain

Workshop Objective – Evaluate and Improve Standards Approach

Q: Commercial vs. DoD Responsibilities

Q: How does DoD envision this working across part types (e.g., COTS, commercial, FPGA, CIC)?

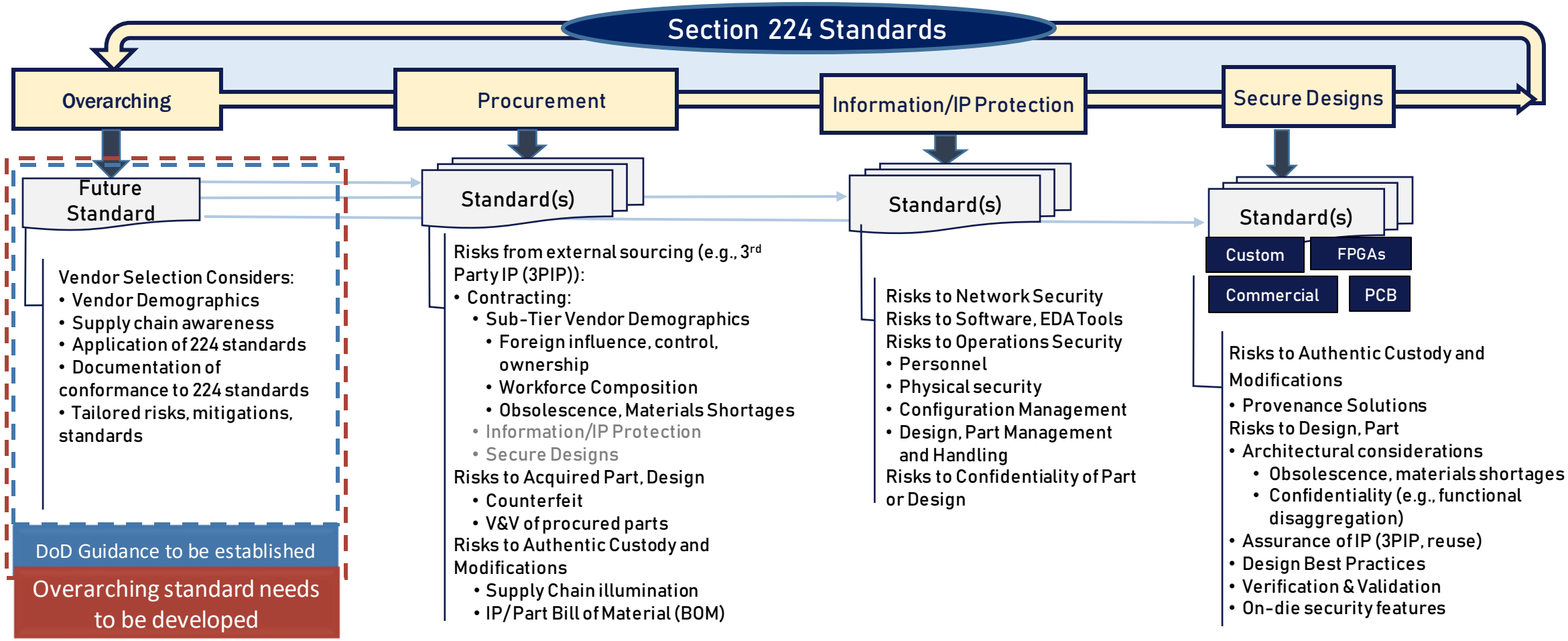
- The intent is that commercial entities execute commercial standards, while DoD unique requirements are limited to the DIB to the extent possible (see graphic)
  - In DoD parts that include both commercial and DoD unique elements (e.g., heterogeneous packages, SoC, etc.) functional decomposition is used



Commercial entities execute commercial standards; DoD unique requirements limited to DIB to extent possible

Approach: Adopting and Establishing Standards

3PIP: Third Party Intellectual Property EDA: Electronic Design Automation V&V: Verification and Validation PCB: Printed Circuit Board



Workshop Objective – Recommend and organize standards

Q: Microelectronics Lifecycle

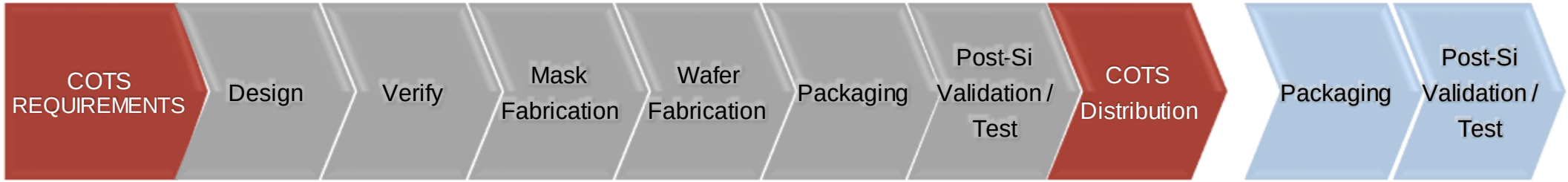
Legend

BLUE	DoD / Program
RED	Industry
GRAY	Industry or DoD Contractor

Q: What do you mean by microelectronics lifecycle?

- The microelectronics development lifecycle begins at requirements and ends at operations and maintenance. Phases that may be performed by commercial *or* DIB elements are shown in gray. Some phases for DoD parts are performed by the DIB (blue).
- This workshop is primarily focused on standards for COTS and Commercial Parts
  - Recommended standards from this activity will be reviewed for applicability, and potentially integrated for DoD specific applications (e.g., CIC, FPGA bitstream).

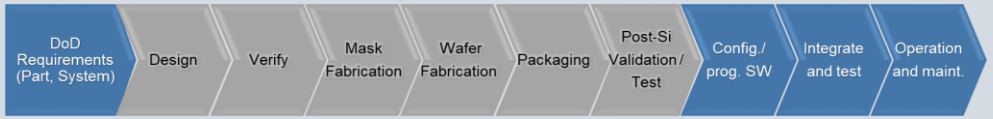
COTS / Commercial Development (not DoD)



Note: May have "minor modifications" to COTS part for DoD reqts. (e.g., package reqts, screening reqts, etc.)

DoD COTS Use

FPGA



Custom Integrated Circuit (CIC)