Microelectronics Standards for DoD

FY20 NDAA Section 224

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

Stephanie Lin
Defense Microelectronics Cross Functional Team

ANSI Workshop
27 July 2022

Motivation & Introduction

NDAA: Standards

NDAA Language:

b) Trusted Supply Chain and Operational Security Standards

1) 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 … that

I. specifies individual features for DoD microelectronics; or
II. otherwise inhibits the acquisition by the Department of securely manufactured, commercially available products.

Standards should address congressionally specified information but should not be military standards

NDAA: Consultation Required

NDAA Language:

b)(2) CONSULTATION REQUIRED.—In developing standards …, the Secretary shall consult with the following:

A. The Secretary of Homeland Security, the Secretary of State, the Secretary of Commerce, and the Director of the National Institute of Standards and Technology.
B. Suppliers of microelectronics products and services from the United States and allies and partners of the United States.
C. Representatives of major United States industry sectors that rely on a trusted supply chain and the operational security of microelectronics products and services.
D. Representatives of the United States insurance industry

Workshop provides forum for representatives from all identified U.S. bodies to provide input

NDAA: Address Needs of USG and Commercial Industry

NDAA Language:

b)(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.

Workshop Objective – Identify standards to support that are applicable to USG and industry

NDAA: Tiers of Trust, Annual Updates

NDAA Language:

b)(3) Tiers of Trust and Levels of Security Authorized — In carrying out paragraph (1), the Secretary may establish tiers and levels of trust and security within the supply chain and operational security standards for microelectronics products and services.

b)(5) Annual Review —Not later than October 1 of each year, the Secretary shall, in consultation with … review the standards … and issue updates or modifications as the Secretary considers necessary or appropriate.

Workshop: primary focus is baseline level of security
Additional levels or tiers may be planned for annual updates

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

Workshop 1

1. Recommend standards or sets of standards that
   a) provide commercially viable mitigations in support of FY20 NDAA Section 224 requirements,
   b) Provide coverage across all phases of the microelectronics development lifecycle
   c) Provide coverage across vendor types
2. Evaluate and improve candidate standards approach
   a) Modular approach for integrated assured supply chain
      a) Methods for determining and sharing compliance to standards across supply chain and to acquirer
      b) 224 related factors that influence sub-tier vendor selection
   b) Requirements development and flow down
   c) Adoption strategy and timelines
   d) Organization of standards

Workshop 2

3. Identify gaps between recommended standards and preferred or necessary supply chain practices
4. Develop path forward to address gaps

Workshop Objective – Recommend and organize standards

Microelectronics Standards – Section 224

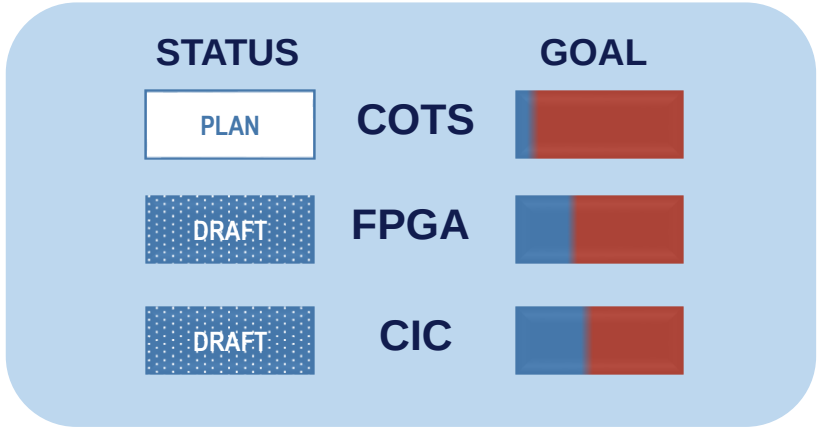
Legend	
BLUE	R&E/CT Deliverable
RED	Commercial Document
GREEN	Other DoD Documentation

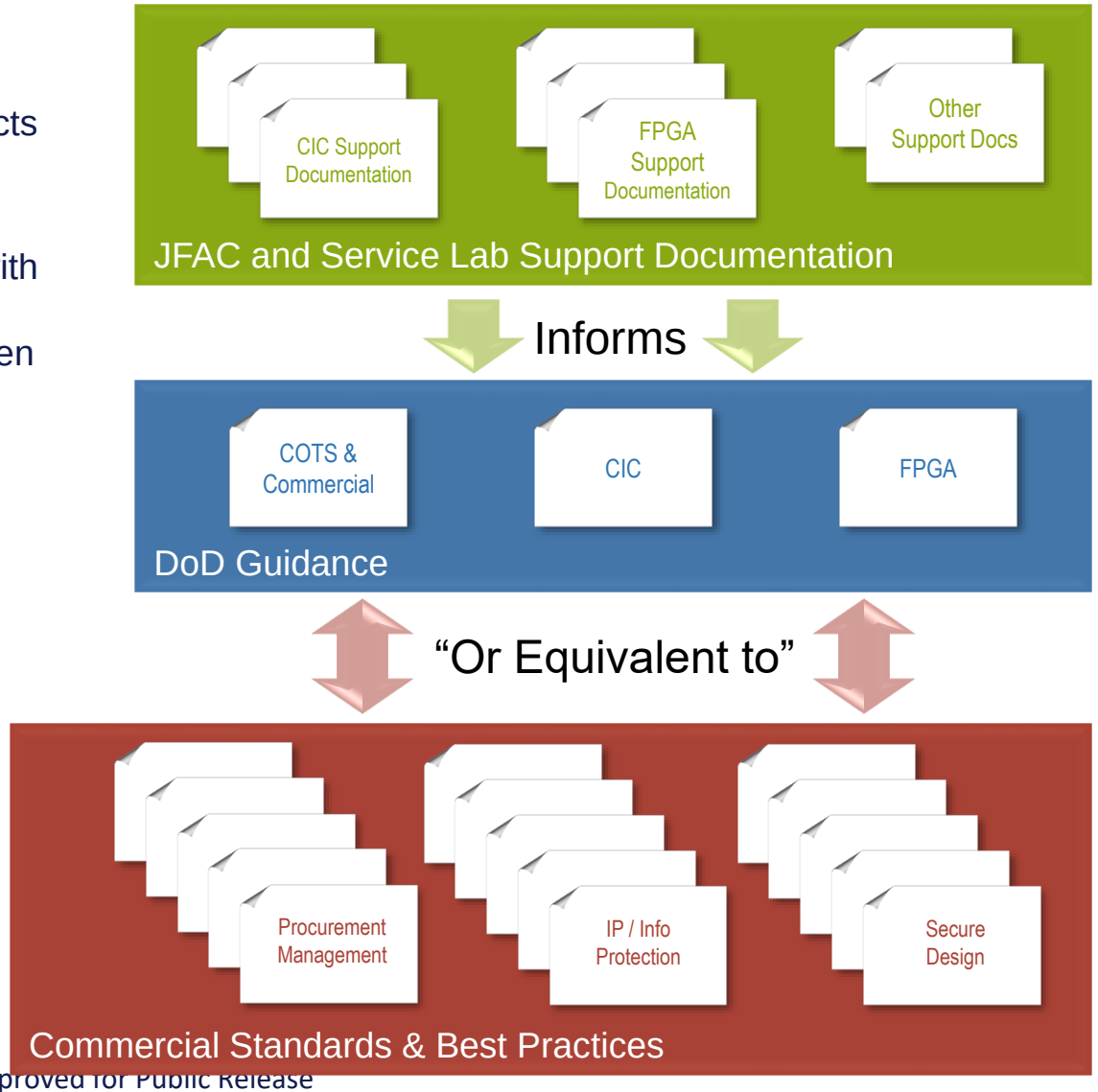
DRIVER

- 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

Approach: Assumptions and Principles

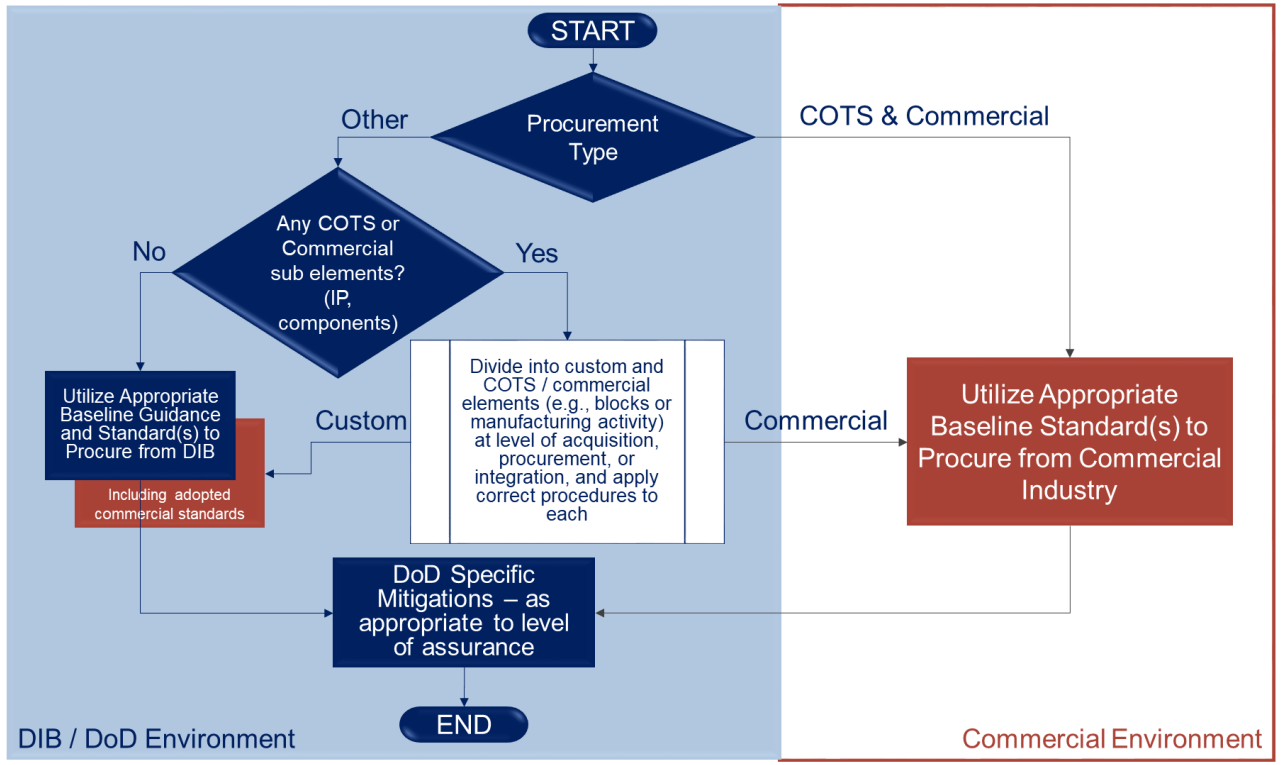
- Workshop focus is COTS and commercial,
  - Choices made will have implications for DoD specific applications (e.g., CIC, FPGA)
- Leverage commercial best practices for baseline level of assurance for COTS and commercial parts
- Execution of DoD specific requirements should be limited to defense industrial base performers to the extent practicable.
- Standards should be
  - Implemented across the microelectronics lifecycle
  - Implemented across tiers of suppliers (commercial, Defense Industrial Base (DIB)) for DoD parts
  - Include a mechanism to assess compliance (e.g., compliance data package(s))
  - Technology agnostic
    - When necessary, multiple standards may be required to address breadth of parts (e.g., digital, analog, RF, radiation hardened, opto-electrical, etc.)

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

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

Identify & Organize Standards

WORKSHOP OBJECTIVE #1

Approach: Categorization of Mitigations

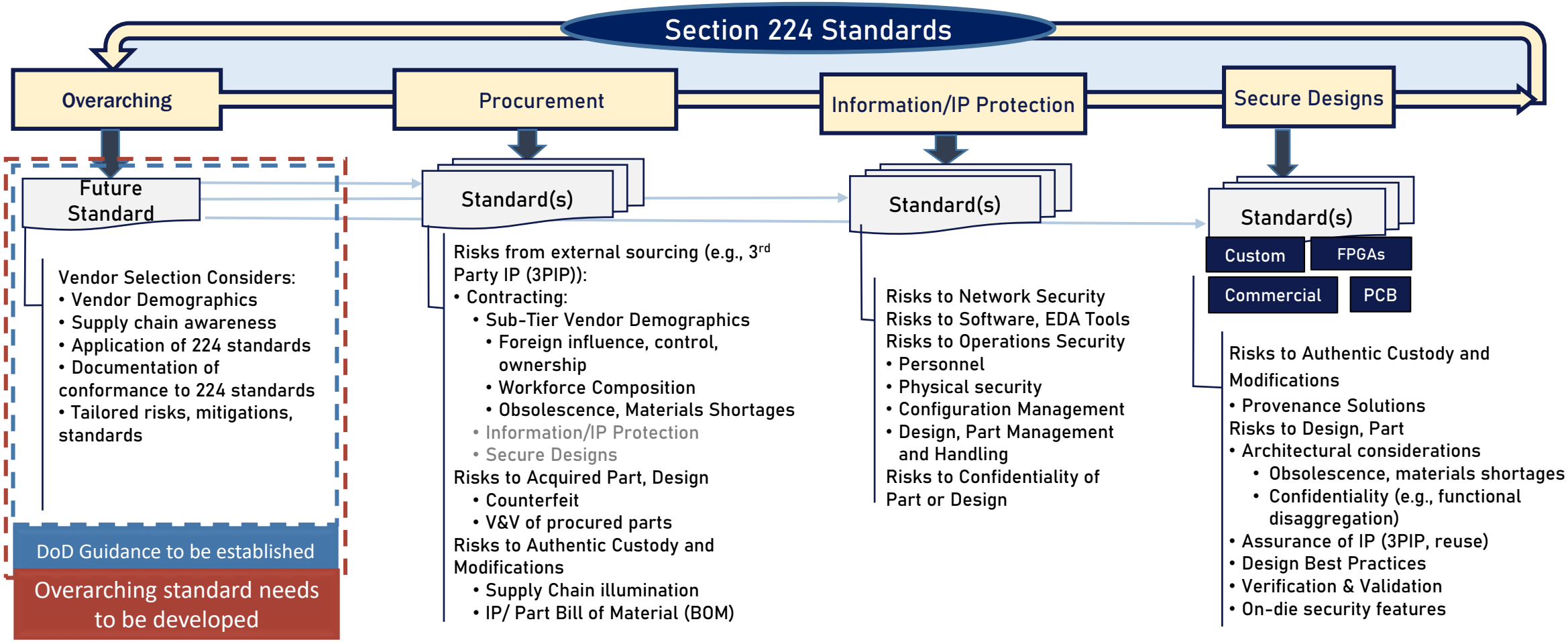
DoD has identified three supply chain practice areas to mitigate microelectronics supply chain risks

Risk Area	Description	Threat
Procurement Management	The process and contractual considerations required for evaluating and defining engagements with external entities for procurements; including the risks/mitigations identified from the other supply chain practice areas. Procurement processes are focused on mitigating risks associated with sourcing IP and parts (e.g., counterfeit, DMSMS), and should include considerations for vendor demographics as identified in FY20 NDAA Section 224 (e.g., company ownership, location, workforce composition)	C, I, A
Information and IP Protection	Risks attributed to the confidentiality of intellectual property and information not intended for public dissemination. May overlap with other supply chain practice areas. Processes are focused on mitigations associated with networks and personnel.	C, I
Secure Design	Design practices to improve assurance (e.g., verification and validation), manage risk when the part is outside vendor or user control, and address supply chain volatility (e.g., open architecture or modularity). May overlap with other supply chain practice areas.	C, I, A

Workshop Objective – Evaluate and Improve Standards Approach

Approach: Adopting and Establishing Standards

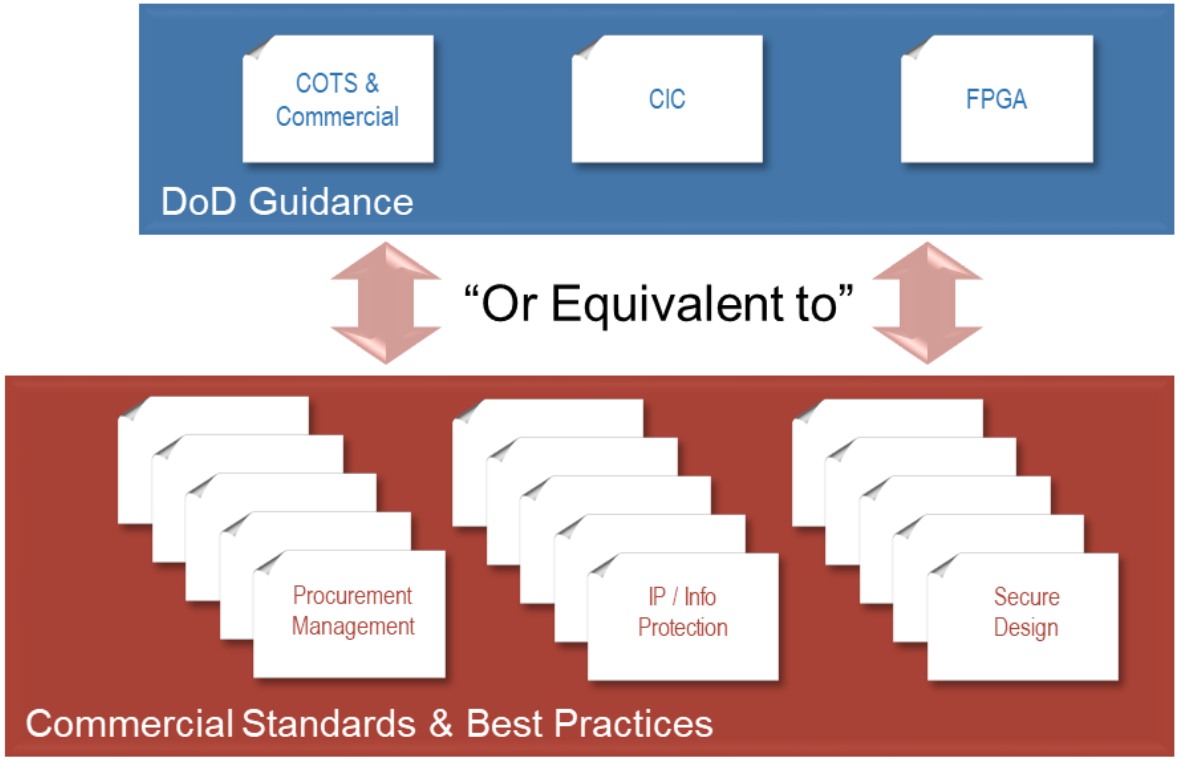
3PIP: Third Party Intellectual Property EDA: Electronic Design Automation V&V: Verification and Validation PCB: Printed Circuit Board



Workshop Objective – Recommend and organize standards

Q: How Many Standards?

Q: How many standards will be adopted? Which ones?	• DoD is utilizing ANSI workshop to evaluate and populate DoD assurance approach with commercial standards across multiple categories.
	  • Multiple standards could be identified to collectively address DoD needs
	  • A single standard could support multiple DoD use cases (e.g., COTS, FPGA)
	  • Etc.



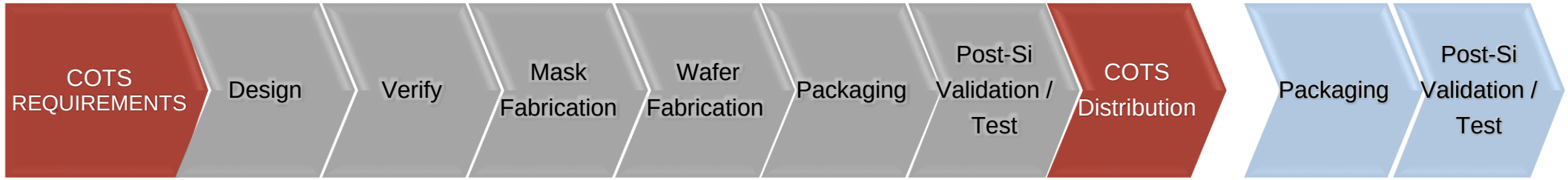
Q: Microelectronics Lifecycle

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).

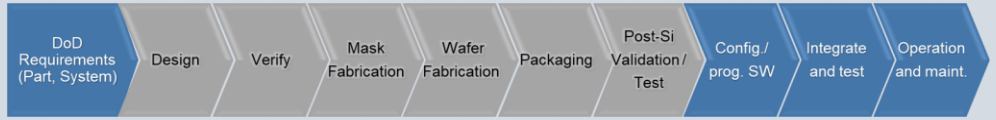
COTS / Commercial Development (not DoD)



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)

Frequently Asked Questions

Legend	
BLUE	R&E/CT Deliverable
RED	Commercial Document

Q: Is Microelectronics Quantifiable Assurance (MQA) the same thing as the response to FY20 NDAA Section 224?	• No. MQA draft standards guidance was developed in response to FY20 NDAA Sec 224. However (a) extension to COTS and Commercial ME is needed, (b) ANSI engagement may identify commercial standards for use in CIC and FPGA to satisfy some DoD needs (e.g., design best practices, verification and validation, etc.)

Q: Is a separate risk analysis required for all microelectronic parts in my DoD system?	• This is program and requirements dependent COTS and commercial parts. The 224 standards are intended to represent a baseline level of assurance for these components. The underlying analysis is considered during establishment of the standards (i.e., now) and updated annually by DoD.
Q: What about FY21 NDAA Section 841? (Printed Circuit Boards (PCBs))	• PCB Executive Agent is responsible for response to Congress • PCB Executive Agent working towards update of IPC 1791 to satisfy NDAA requirement • Overall standards approach is process oriented and expected to be able to support PCB response and standard(s)
Q: Are 224 standards applied to all microelectronics components	• Yes

Evaluate and Improve Candidate Standards Approach

WORKSHOP OBJECTIVE #2

Risk Management and Requirements Development

	Risk Analysis Task	Status	Notes
1	Determine Applicability	Complete	Focus: COTS and commercial Technology agnostic
2	Analysis	**Workshop Activity**	DoD responsibility
2a	Risk analysis – identify risks, vulnerabilities, threats	Complete	Utilize CIA triad
2b	Risk management – select, apply mitigations	**Workshop Activity**	DoD responsibility. Workshop solutions may require additional mitigations (DoD unique or commercial expectations)
2c	Evaluation – assess residual risk	**Workshop Activity**	
3	Execution	N/A	Outside the scope of the workshop Completed per design, part, program
3a	Demonstrate compliance		

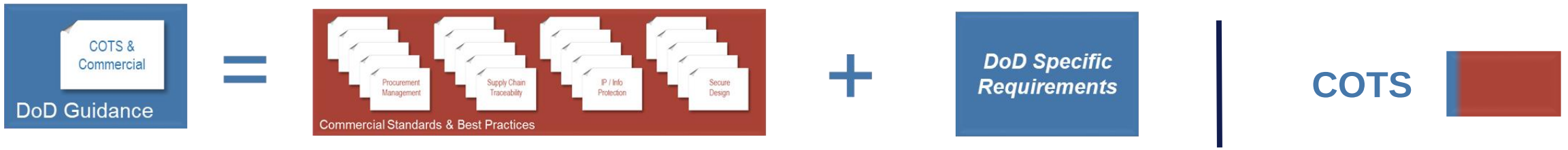
Workshop Objective – Recommend and organize standards

Q: Commercial vs. DoD Requirements

Q: How does a commercial standards approach align to DoD specific requirements?

- DoD guidance will include both use of commercial standards and DoD specific requirements (intended for DIB)

1. This workshop is focused on identifying appropriate standards
   - Satisfy FY20 NDAA Sec 224, address microelectronics assurance
2. This workshop provides preliminary identification of gaps to DoD needs
   - Workshop 2 (Oct 2022) develops plans to close those gaps



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

Responsibility: Requirements, Risk Analysis

		Responsibility for		
	Reqt Received	Risk Analysis	Reqt Development	Reqt Flow Down
DoD	FY20 NDAA Sec 224	Updated annually (FY20 NDAA Sec 224)	Primary responsibility • Consulting with USG, industry, SDOs (including ANSI workshop)	TBD. For consideration: • Program requirements • DoD policy / guidance • DFARS update
Program (or primary acquirer)	TBD. For consideration: • Program requirements • DoD policy / guidance • DFARS update	• Per DoDI 5200.44, 5000.83 • Separate analysis is not expected for each COTS part	• Execute 224 contracts requirements, including flow down; and • Supplement 224 contracts requirements in accordance with program risk analysis	• Flow down 224 contracts requirements and any relevant supplemental requirements
Performers	• 224 contracts requirements and any relevant supplemental requirements received from next-higher acquiring entity	• Performer may perform additional risk analysis to tailor (supplement) requirements for themselves and/or flow down	• Execute 224 contracts requirements including flow down; and • Performer may tailor (supplement) 224 contracts requirements	• Flow down 224 contracts requirements as required; and • Performer may flow down supplemental requirements

Workshop Objective – evaluate and improve candidate approach

Performers should flow down 224 requirements and may add vendor or product specific assurance requirements

Modular Implementation

- Application of standards is intended to be modular
- Interlocked supply chain practices, when utilized across tiers of performers culminate in an integrated assured supply chain
- Evidence of compliance is passed through the supply chain

Workshop objective – Recommend acceptance criteria for compliance

Interlocked application of 224 standards yields integrates assured supply chain

Q: How is Approach Integrated Across Lifecycle

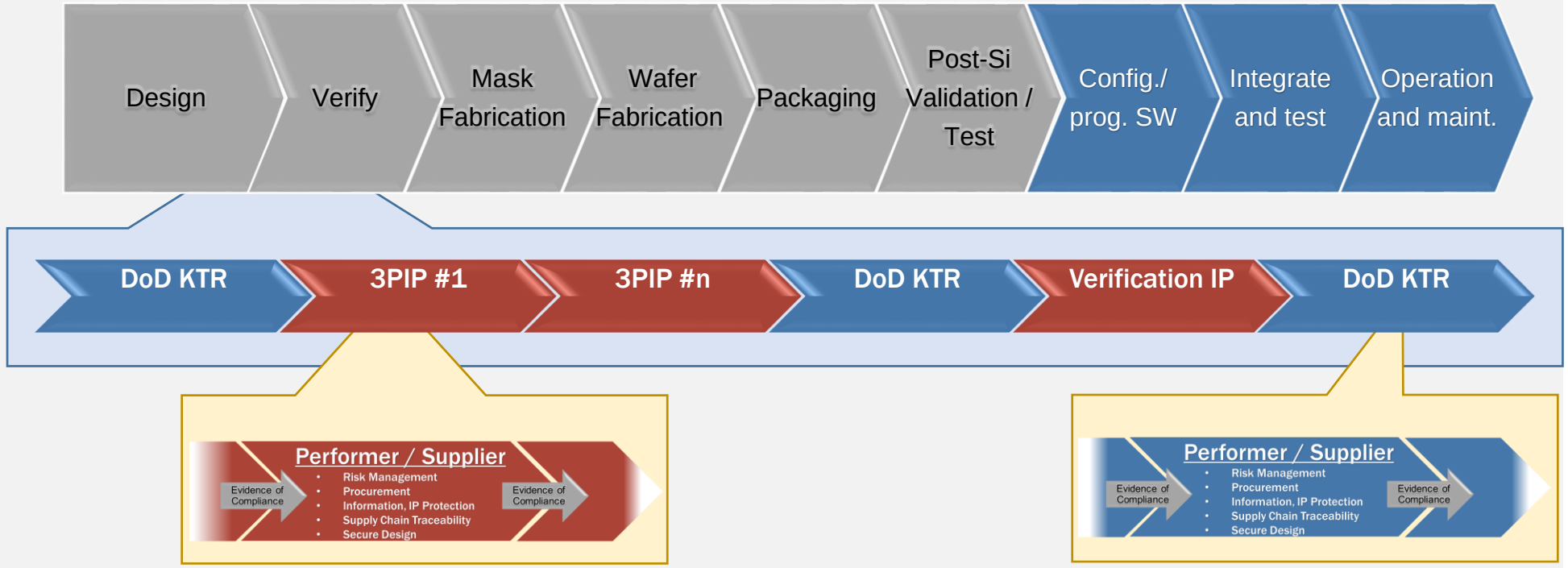
Q: How is the modular approach utilized across the supply chain	• Acquirer flows down requirements (e.g., 224 standards) and considers vendor demographics for assured microelectronics • Performers execute standards, provide compliance data packages to their customer (repeats across tiers of vendors)

3PIP: Third Party Intellectual Property KTR: Contractor Post-Si: Post Silicon

Baseline requirements flowed down to performers across the lifecycle

Multiple vendors may support a single lifecycle phase

Each vendor applies appropriate standards to its activities



Interlocked application of 224 standards yields integrates assured supply chain

224 Standards – Influencing Vendor Selection

- Assurance factors in selecting microelectronics products and service providers:
  - Vendor Demographics
  - Application of 224 standards
    - Availability of compliance information for 224 standards
  - Supply chain illumination and awareness
  - Tailored risks, mitigations, standards

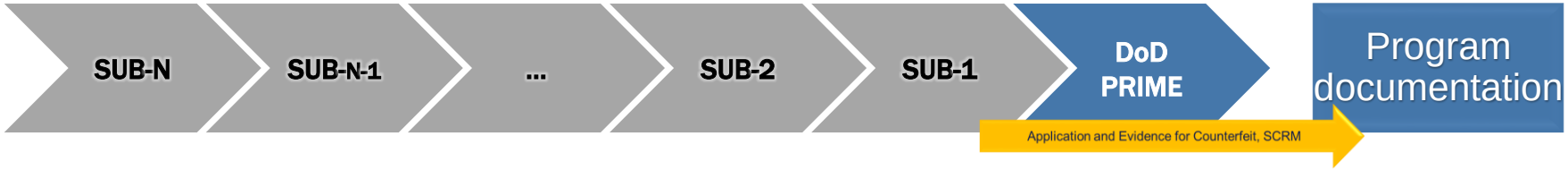
Required by FY20 NDAA Sec 224

- DoD programs should consider non-compliance to 224 standards in their evaluation of technical risk.

Workshop Objective – evaluate and improve candidate approach

Q: What are the Expectations for Adoption?

TODAY: SCRM and counterfeit policies and regulations provide a baseline to ensure authenticity of DoD microelectronics and to ensure health and security of suppliers. DoD standards approach seeks to extend assurance via application of standards.



GOAL: Integrated assured supply chain, with all tiers of suppliers from design utilizing 224 standards.

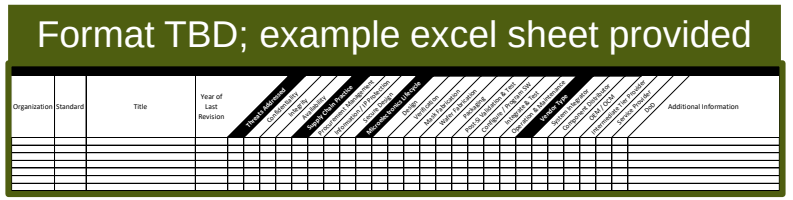
INTERIM: What is the expectation for adoption rate? What are the challenges to rapid adoption? What could be done to overcome those challenges?

Workshop Objective – Recommend adoption strategy

Breakout: Microelectronics Standards Evaluation

1. Recommend standards or sets of standards that
   a) provide commercially viable mitigations in support of FY20 NDAA Section 224 requirements,
   b) Provide coverage across all phases of the microelectronics development lifecycle
   c) Provide coverage across vendor types
2. Evaluate and improve candidate standards approach
   a) Modular approach for integrated assured supply chain
      a) Methods for determining and sharing compliance to standards across supply chain and to acquirer
      b) 224 related factors that influence sub-tier vendor selection
   b) Requirements development and flow down
   c) Adoption strategy and timelines
   d) Organization of standards

Format TBD; example excel sheet provided



Workshop Objective – Recommend and organize standards
Workshop objective – evaluate and improve candidate approach