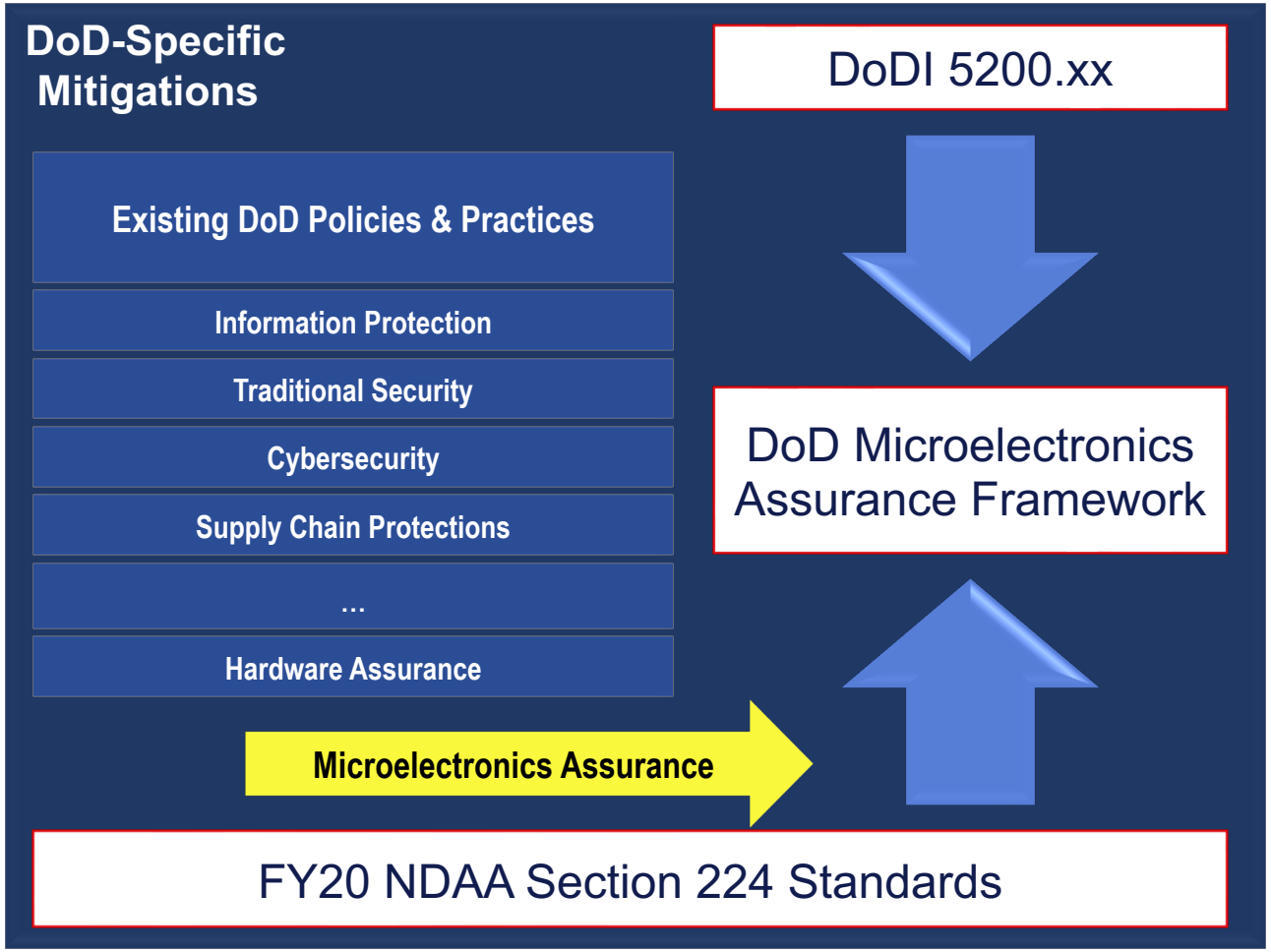
USD(R&E)

Microelectronics Policy, Standards and Guidance

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

Microelectronics Reliability and Qualification Workshop
9 Feb 2023

DoD Microelectronics Assurance Framework



GOAL: Access and assurance to best-available microelectronics to support resilience of DoD systems

DoD Microelectronics Assurance Framework (MAF) provides programs with implementation guidance to address microelectronics-specific risks

- Supports breadth of DoD microelectronics
  - Component customizability – Commercial off the Shelf (COTS) through Custom Integrated Circuit (CIC)
  - Technology generation – legacy, State of the Practice (SOTP), State of the Art (SOTA)
  - Technology type – digital, analog, RF, radiation hardened, opto-electronic, etc.
  - Expand Assurance Toolbox – trusted suppliers when available, or alternative methods when needed
- Programs utilize risk-based decision-making through established methods and practices (e.g., Systems Security Engineering (SSE), risk analysis)
- Programs manage risk across the microelectronics development lifecycle

Approach for assured microelectronics developed after top-down evaluation of policies, use cases

Access and Assurance for Microelectronics Policy, Standards and Guidance

- DoDI 5000.83, *Technology and Program Protection to Maintain Technological Advantage*
  - Requires risk-based measures to protect systems and technologies from adversarial exploitation and compromise
  - Requires program use of SSE methods
- DoDI 5200.44, *Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)* update includes
  - Applies to a subset of components in "applicable systems"
  - Risk management including TSN process, tools and techniques
  - Requirement for trusted supplier using trusted processes accredited by the Defense Microelectronics Activity (DMEA) for ASICs
  - USD(R&E), in coordination with the USD(A&S), establishes processes and procedures for accessing assured microelectronics in accordance with Section 231 of Public Law 114-328.
- FY17 NDAA Section 231 of Public Law 114-328, Strategy For Assured Access To Trusted Microelectronics
  - DoDI 5200.XX, *Access and Assurance for Microelectronics, TBD*
  - Describing how Department of Defense entities may access assured and trusted microelectronics supply chains for the Department of Defense systems
- FY20 NDAA Section *224,Trusted Supply Chain and Operational Security Standards*,
  - Directs the Secretary of Defense establish trusted supply chain and operational security standards for the purchase of microelectronics products and services by the Department
- DoD Microelectronics Assurance Framework
  - Provides programs with implementation guidance to address microelectronics-specific risks

Comprehensive policy, guidance, standards strategy for access and assurance of microelectronics

DoDI 5200.xx – Access and Assurance for Microelectronics

DRIVER

- OUSD(R&E) response to FY17 NDAA Section 231(d)
  - "… shall issue a directive for the Department of Defense describing how Department of Defense entities may access assured and trusted microelectronics supply chains for Department of Defense systems"

PLAN

- Policy to address access and assurance for microelectronics
  - Access – requirements analysis to inform investments, improve access and promote procurement efficiencies
  - Assurance – evaluate risk and implement mitigations for commercial and custom microelectronics utilized in DoD applications
- Development effort includes mapping to other relevant DoD policies to ensure appropriate coverage
- Policies cannot conflict with each other, and do not simply repeat each other
  - DoDI 5200.44 requires use of DMEA accreditation for ASIC product and services

STATUS

- Current draft incorporates comments from early coordination within OUSD(R&E) and DMCFT
- Up next: informal coordination

DoDI 5200.xx will contain high-level requirements for access and assurance for microelectronics

Microelectronics Standards – Section 224

Legend

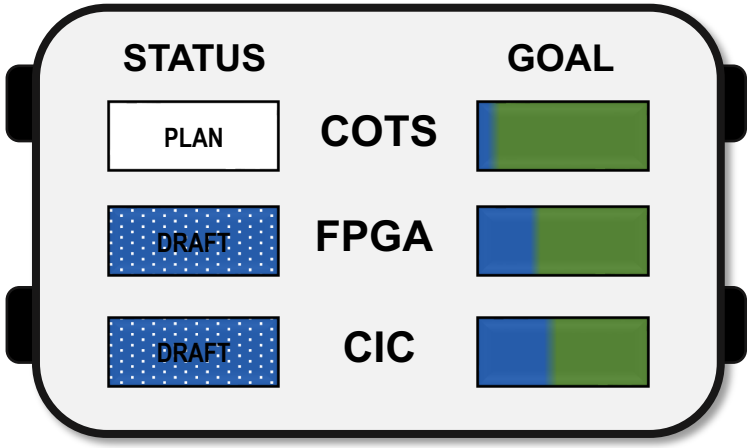
BLUE	R&E/CT Deliverable
GREEN	Commercial Document
GRAY	Other DoD Documentation

DRIVER

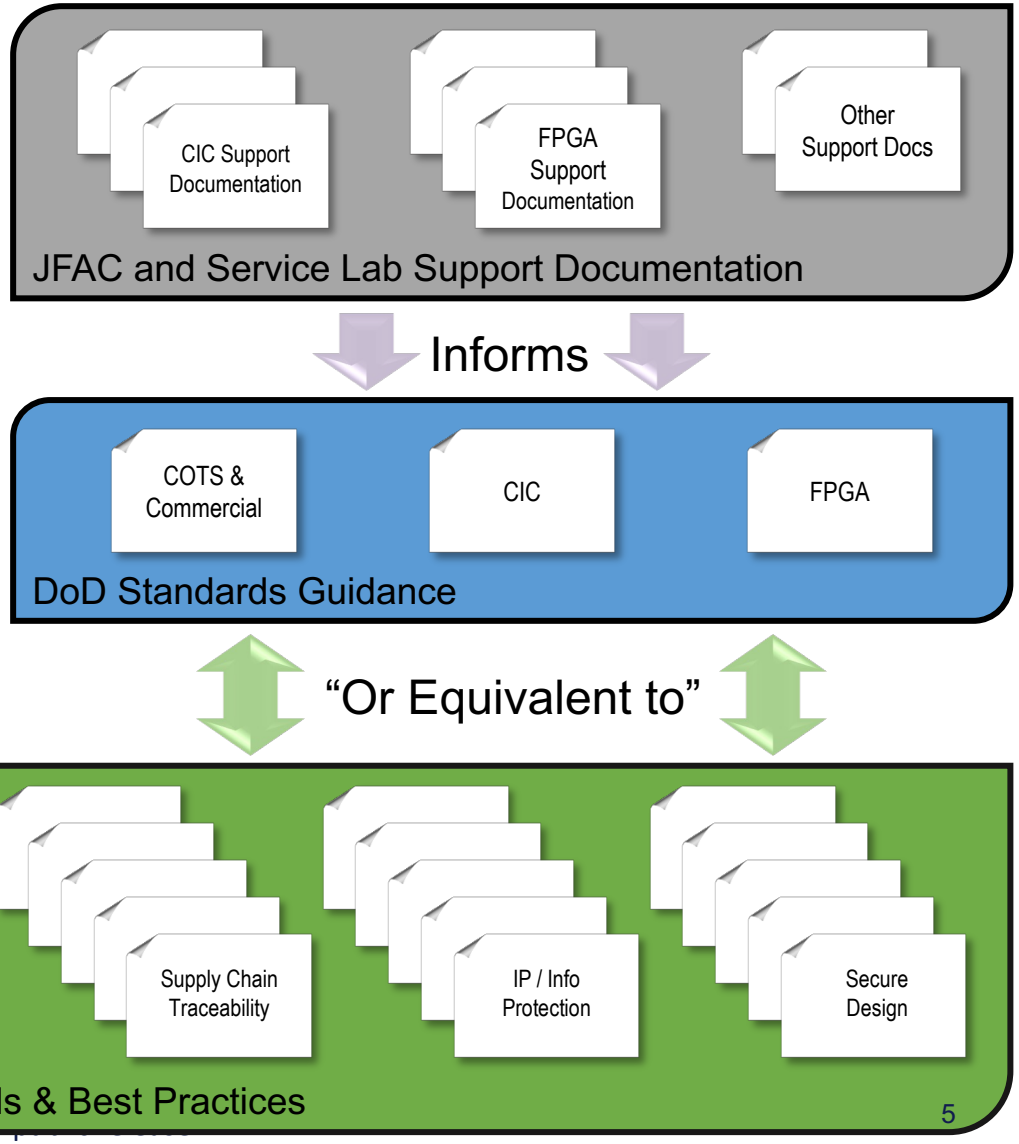
- FY20 NDAA Sec 224 – "… shall establish trusted supply chain and operational security standards for the purchase of microelectronics products and services by the Department"

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



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

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

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

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

Microelectronics Guidance – DoD Microelectronics Assurance Framework

DRIVER

- DoD Microelectronics Assurance Framework (MAF) provides programs with implementation guidance to address microelectronics-specific risks

PLAN

- MAF guidance:
  - Provides program-specific analysis across the microelectronics development lifecycle
  - Guides program in identification of microelectronics ecosystem threats
  - Guides program in identifying and evaluating mitigations to microelectronics ecosystem threats
  - Guides program in evaluating microelectronics component security risk

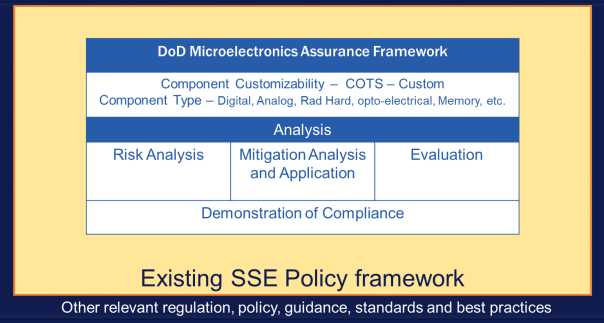
STATUS

- Basic framework is established
- Up next: alignment efforts for key elements (e.g., acquisition models, system engineering V timeline, levels of assurance, etc.)

DoD Microelectronics Assurance Framework guides DoD acquisition programs to manage the integrity and confidentiality of their microelectronics components, resulting in a level of assurance commensurate with DoD acquisition program requirements.

It utilizes Systems Security Engineering (SSE) activities to identify microelectronics risks and vulnerabilities, and to apply appropriate mitigations across the development lifecycle.

It leverages standards and evidence, including supplier data, to generate quantitative and qualitative metrics, and informs the program about its microelectronics security risks.



DoD MAF provides programs guidance to manage microelectronics specific risks

DMEA Trusted Supplier Network

Q: How will trusted suppliers be addressed in policy?

Use of DMEA accreditation for ASIC products and services is explicitly addressed, by a policy statement in DoDI 5200.44 .

- DoDI 5200.44, *Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)*
  - Requirement for trusted supplier using trusted processes accredited by the Defense Microelectronics Activity (DMEA) for ASIC products and services

- DUSD R&E Statements re: Trusted Foundry
  - "The TF model has proven effective over many years of supplying secure access"
  - "to date, there is no known substitute for this capability"
  - "Through recent arrangements, DoD's national security needs are being addressed through the TF model for technology nodes… to 12 nm"

Trusted Foundry Attributes

Accreditation methodology leverages USG certifications and commercial standards.

Security/quality/configuration processes to assess integrity of people and processes for a range of technologies critical to DoD

Design agnostic approach that leverages commercial microelectronics suppliers

Ensures Secure chain-of-custody across lifecycle

Defense Counterintelligence and Security Agency (DCSA) Facility Clearance, Personal Clearances as needed, Commercial Quality Standards, DMEA approved ME plan

Network of Trusted Suppliers for Design, Fab & Test

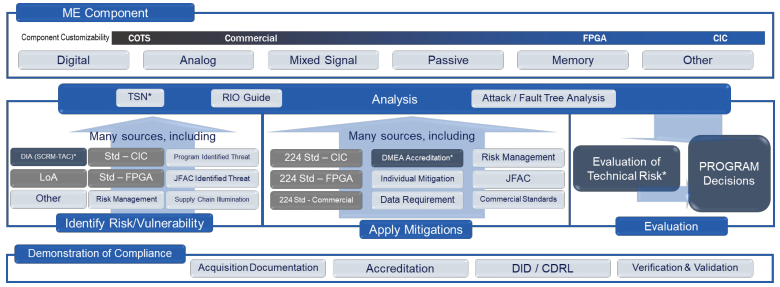
Trusted Packaging Facility

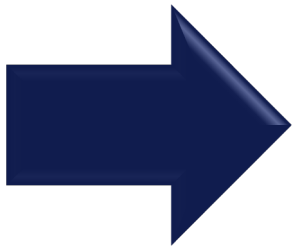
The Trusted Foundry model has served as an effective assurance method for DoD microelectronics since 2004

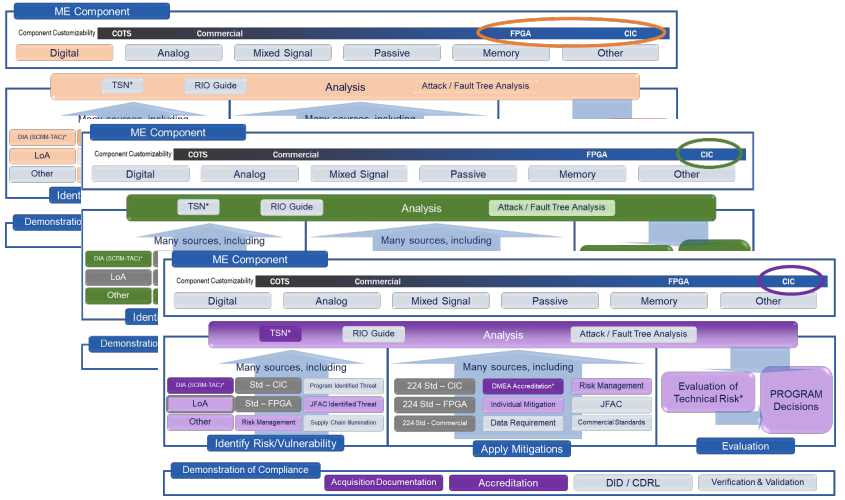
MAF (Guidance) vs. Implementation Solution

MAF:

- The MAF construct was developed because of an understanding that policy must be flexible enough to support adaptive acquisition and technical solutions (current and future) for access and assurance of microelectronics



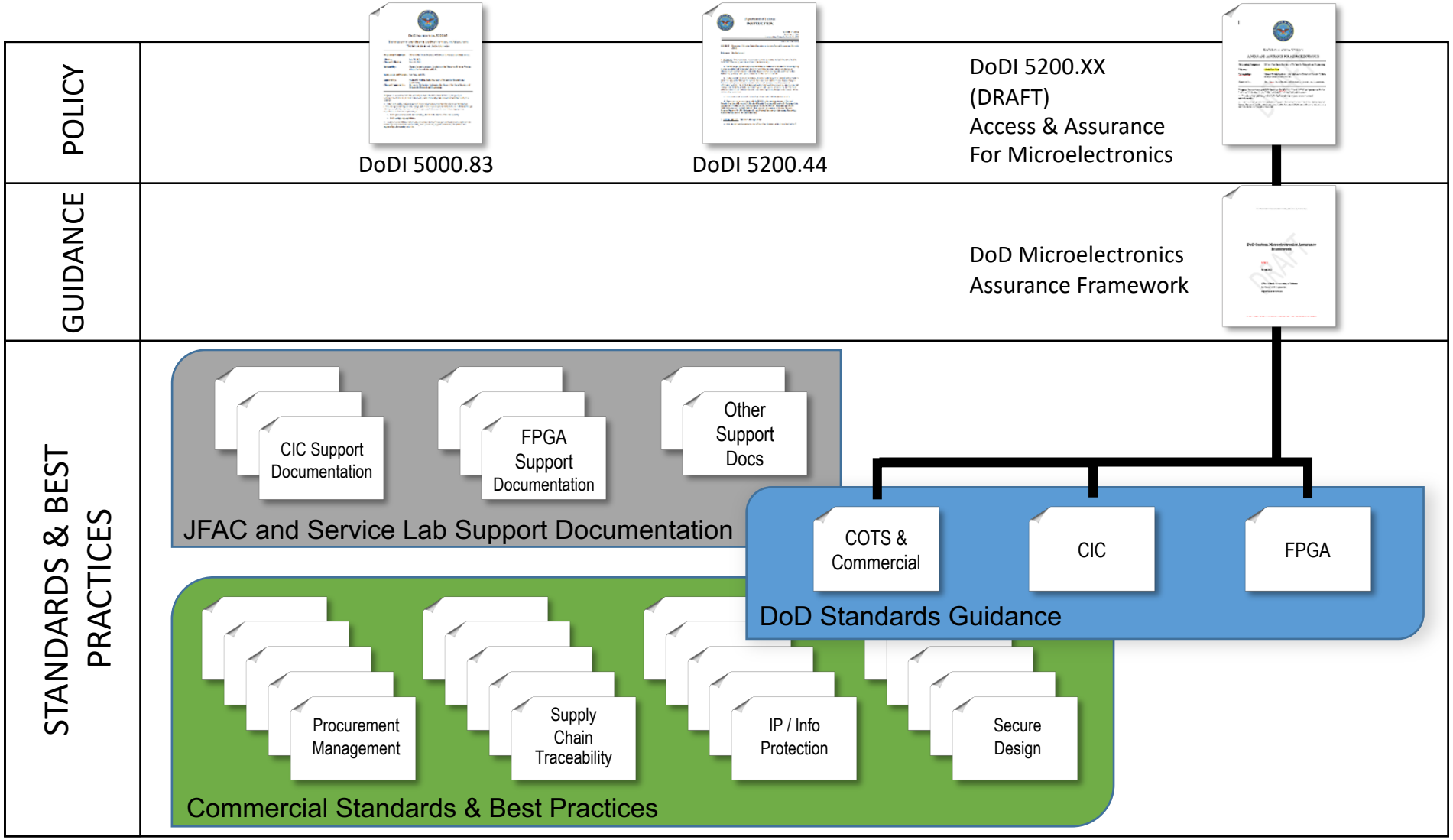




DoD MAF can be satisfied in multiple ways, based on program use case

Summary

- DoD Microelectronics strategy includes policy, standards, and guidance to ensure access and assurance across the breadth of DoD microelectronics



Legend	
BLUE	R&E/CT Deliverable
GREEN	Commercial Document
GRAY	Other DoD Documents

Comprehensive policy, guidance, standards strategy for access and assurance of microelectronics