USD(R&E)

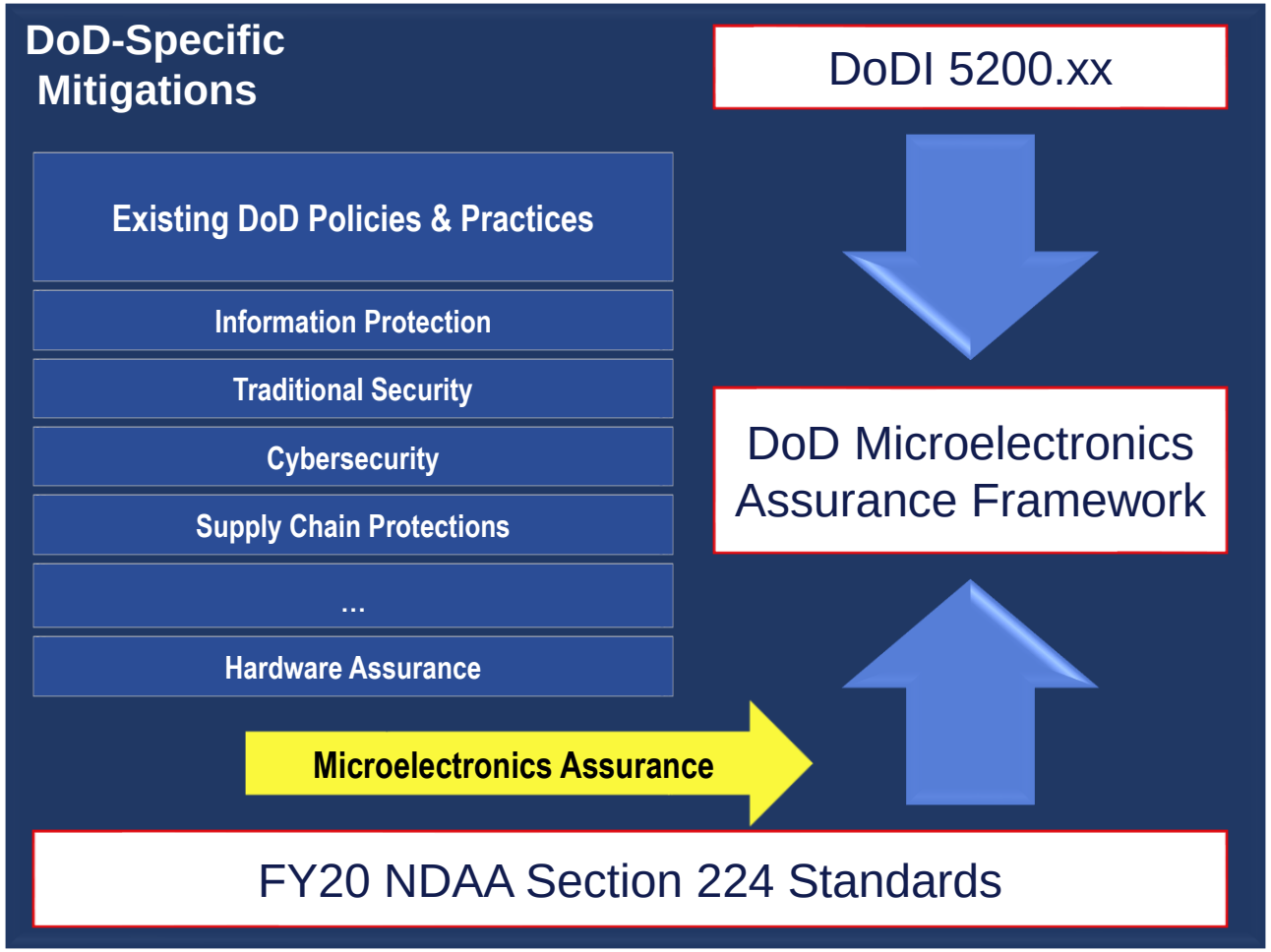
DoD Microelectronics

Policy, Standards and Guidance

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

NDIA Electronics Workshop
31 Aug 2022

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-electrical, etc.
  - Expand Assurance Toolbox – trusted suppliers when available, or alternative methods when needed (e.g., microelectronics quantifiable assurance, zero trust)
- 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

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

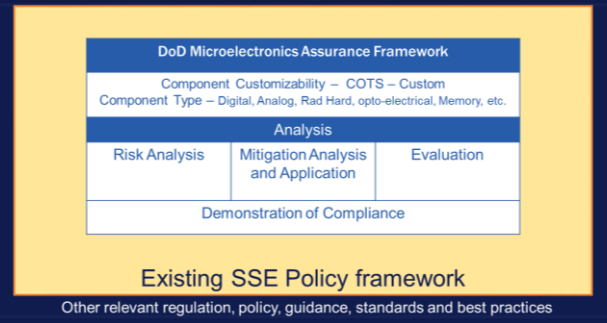
STATUS

- 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

Microelectronics Quantifiable Assurance

DRIVER
- Develop methodology to evaluate and manage risk of DoD access to SOTA technology nodes via commercial sources
- Data driven approach to mitigate evolving threats and improve resilience
- DUSD (R&E) “DoD will require multiple tools in its toolbox”

PLAN
- For each threat, microelectronics risk is measured against criteria established for selected level of assurance
  - Utilizes data already generated in development and manufacture of microelectronics
  - Employs commercial best practices as practicable
- Program manages risk via DoD MAF, with draft MQA guidance serving as sources for threats, mitigations

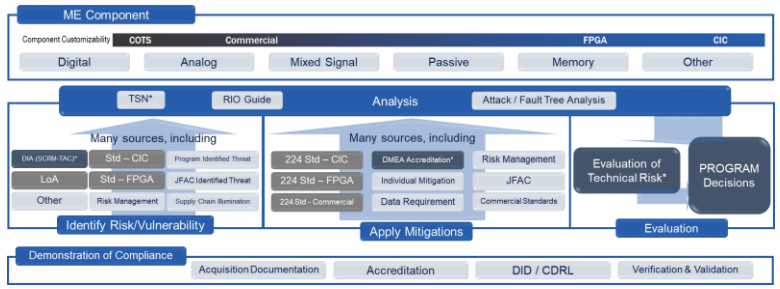
STATUS
- DUSD(R&E) “MQA is a proposed methodology that has not been verified or validated”
- “OUSD(R&E) leadership has recently formed a Red Team … to evaluate the MQA methodology, the draft standards, the MQA pilots, … for its potential to assure microelectronics hardware for the DoD and IC.”
- T&AM and JFAC are working with multiple pilot programs, including RAMP, to evaluate the application of MQA standards and methods
- MQA standards guidance are in an iterative update cycle. Rev 4.0 released April 2022

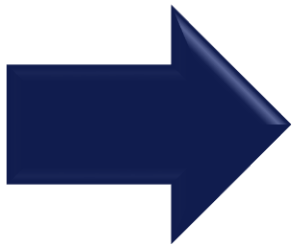
MQA provides important tools in DoD microelectronics assurance toolbox

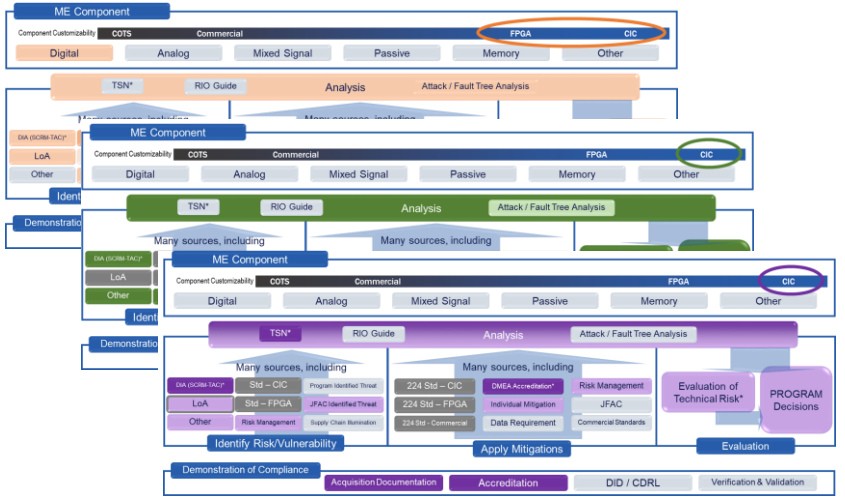
MAF (Guidance) vs. Implementation Solution

MAF (*vs MQA*):

- 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