Department of the Air Force

Integrity - Service - Excellence

NDAA 2023 Mandated Independent Review of USD (R&E) Microelectronics Quantifiable Assurance Effort

UNITED STATES AIR FORCE
CHIEF SCIENTIST

Dr. Victoria Coleman
AF/ST
3 August 2023
Version 1.0

DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited

Outline

- Congressional Direction
- Section I: Executive Summary
- Section II: Findings
- Section III: Analysis
- Section IV: Recommendations
- Acknowledgements, Definitions & Acronyms

DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited

Congressional Direction

- NDAA FY 2023 Report 117-130, July 18, 2022: pages 85-6
- *The committee is aware that the Department of Defense's (DOD) present microelectronics security strategy rests on a decision to partner with leading commercial semiconductor companies to understand, quantify, further develop, and codify in standards the existing processes used to protect the integrity and confidentiality of intellectual property (IP) in commercial integrated circuits. This approach, referred to as quantifiable assurance, rests on data and processes that are inherent in the commercial processes at microelectronics design and manufacturing facilities through comprehensive instrumentation and data analysis of each step in design and production.*
- *Commercial fabless semiconductor companies, in partnership with their foundry manufacturers, use these quantifiable assurance processes today for quality control and IP protection. These commercial companies manufacture millions of chips a day with very high yields in a very competitive industry, and thus have demonstrated these processes are economically viable. The Department is exploring these processes in partnership with a commercial foundry to manufacture a chip for its next-generation Global Positioning System (GPS) receivers (known as the M-Code GPS User Equipment (MGUE)). Between this MGUE program of record precedent and the massive use of these quantifiable assurance methods in commercial industry's quality control processes, the committee is confident that the DOD can develop an approach with industry partners that meets its security needs without incurring unsustainable costs or threatening the commercial viability of its industry partners.*
- [continued on next slide]

Congressional Direction

- ***The committee believes that this approach for quantifiable assurance is more viable in the long run, and more closely aligns with commercial practices, than traditional approaches for dedicated Trusted Foundries. The committee understands that the benefit of this methodology is that it enables hardware designs to be processed through commercial manufacturing facilities, at high volume and in compliance with the International Traffic in Arms Regulations without requiring classified facilities, equipment, processes, or personnel with security clearances. However, the Department has asserted to the DOD Inspector General in a recent letter that it is not possible to create a plan for transition to a quantifiable assurance model until the methodology has been "proven to effectively provide required levels of protection equal to or greater than what is currently provided by the [Trusted Foundry] model."***

- ***Given the differences in the approaches and the fundamental challenge in proving any security model, the committee is concerned that the DOD is creating an insurmountable hurdle that is discouraging an adequate risk trade-off assessment for the quantifiable assurance approach. Therefore, in order to ensure that a diversity of views are available to inform decisions in this critical and complex matter, the committee directs the Chief Scientist of the Air Force to conduct an independent review and lead supporting efforts for the quantifiable assurance effort underway in the Office of the Under Secretary of Defense for Research and Engineering (USD R&E). The committee directs that these efforts and the review of the Department's approach to quantifiable assurance include: (1) Examples of existing quantifiable assurance standards from industry and international partners and their effectiveness; (2) Mapping of data sources that would provide this information to process workflows in order to identify any gaps in data, or data sources; (3) Leveraging of the Air Force's MGUE experience; and (4) Formalization of a threat model and threat vectors against which quantifiable assurance and other security models shall be assessed. In conducting the review and development, the committee expects the Chief Scientist of the Air Force to include participation and input from entities with expertise in commercial implementations of quantifiable assurance and in threat assessment. The committee directs the Chief Scientist to provide a briefing to the congressional defense committees on this effort not later than June 1, 2023.***

Section I:

EXECUTIVE SUMMARY

Review Approach

- The Chief Scientist of the United States Air Force assembled a panel of 27 experts across government, the defense industrial base, the semiconductor industry and academia.
- Non-government panelists were appointed as Special Government Employees for the purposes of the review.
- The panel was subdivided in five subpanels focused on:
  - MQA status, Standards, Threat Model, Trusted Foundry, and Implementation Plan.
- The panel convened for four in person meetings, received briefings, and held discussions.
- USD(R&E) supported the work of the panel by providing materials, briefings and advisory expertise.
- The present brief represents consensus amongst the panel members.

The Key Questions

- What are the national security implications of using the commercial supply chain?
- What are the risks entailed?
- How can we mitigate these risks in a practical way?
- Will the risk reduction be enough?
- How are we going to implement in practice a viable risk reduction regime?

BLUF

- The vast majority of the microelectronics embedded in DoD systems are commercial off-the-shelf components (COTS). Custom integrated circuits (CICs) are developed as a last resort to meet unique DoD functionality, performance or security needs.
- The microelectronics needs of the DoD can only be met by continuing to access the commercial supply chain.
- However DoD unique requirements necessitate the creation and application of additional measures to ensure parts that are procured from the commercial supply chain are suitable for deployment to DoD systems. Today it is not possible to meet these additional requirements.
- While DoD's trusted suppliers are a key part of the defense industrial based, the vast majority of DoD microelectronics purchases are not using the trusted supply chain.
- Trusted Foundry (TF) which is mature and Microelectronics Quantifiable Assurance (MQA) which is in development, are two approaches that can be used to meet different aspects of these requirements.
- There has been much debate about the virtue of each and a false dichotomy between TF and MQA. The Panel believes that a combination of TF and MQA is necessary in order to meet DoD microelectronics needs.

DoD Microelectronics Access Needs

- DoD microelectronics needs encompass State of the Art (SOTA), State of the Practice (SOTP), and legacy semiconductor technologies including silicon CMOS for processing systems and compound semiconductors for sensor, power, and communications systems. There is no single semiconductor process, node or fab that can satisfy all the diverse DoD requirements.
- DoD needs include access to unclassified, classified, and export-controlled microelectronics
- Because of the economics of the semiconductor industry, the DoD cannot maintain dedicated facilities and therefore needs to access the commercial supply chain to meet most of our needs.
- These needs can be met by creating DoD specific overlays on commercial processes.
  - TF is a mature approach that adds security overlays to assure that classified information is not disclosed to unauthorized parties.
  - MQA is an emerging approach that includes independent, data centric checks on commercial processes to provide additional assurance.
- It is in the DoD’s interest to have access to multiple sources of microelectronics components for resiliency and cost competitiveness.

Desired Assurance Properties of DoD microelectronics

- DoD system assurance requirements vary and are dependent on the specific systems within which they are deployed.
- Desired assurance properties are:
  - Confidentiality, meaning that information and intellectual property contained within the device is not disclosed to unauthorized parties.
  - Integrity, meaning that a device will function as intended and is free of either intentionally or unintentionally inserted known vulnerabilities.
  - Availability, meaning that the device is available to perform its function when required to do so for successful DoD system operation.
- Access is the overarching requirement, meaning the ability of the DoD to obtain parts in a timely, cost effective manner to satisfy programmatic needs.

DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited

What is Trusted Foundry?

- TF is an overlay on a commercial flow offered by GlobalFoundries that offers protection against unauthorized disclosure of classified information (including data and government intellectual property) to unauthorized persons.
- TF originated from the sale of IBM's semiconductor business to GlobalFoundries in 2014 (in fact IBM paid GlobalFoundries $1.5B to "buy" the business - an indication of the unforgiving economics of the semiconductor industry).
- It is a mature, regulated process with oversight from DCSA as well as DMEA, a separate DoD security accreditor.
- Enables the commercial manufacturer to run products of any level up to the designated clearance level.
- TF includes a contract to guarantee access and an organization (TAPO) to manage the customer interface, aggregate DoD demand, and provide needed design IP and provide customer support.
- TF is a way for the DoD to ensure that classified information in a device has not been exposed to unauthorized parties. In and of itself, TF does not offer additional assurance.

What is Microelectronics Quantifiable Assurance?

- MQA is an emerging data-centric approach to independently assess integrity across the microelectronics development lifecycle including design and manufacturing. For example:
  - Place and route techniques that prevent or detect trojan insertion.
  - Detection of unexpected delays in the process flow. An unexpected delay might indicate an opportunity for someone to tamper with the lot.
  - Overproduction: did you use my IP without permission?
  - Process control: did you treat my lot differently?
  - Wafer fabrication compromise.
- Semiconductor manufacturers perform meticulous variance checks during manufacturing. MQA seeks to leverage the data created in support of these checks to implement an additional set of independent integrity checks.
- MQA is a way for the DoD to obtain additional assurance on the integrity of a part and its availability to function as desired.

TF and MQA Compared

- MQA applies to the entire lifecycle of microelectronics including design whereas TF focuses on the fabrication stage only.
- MQA and TF have similar objectives, that is to assure that a part is fit for purpose. However, the approach to that objective differs:
  - TF is based on trusting humans.
  - MQA is based on trusting data.
- MQA is primarily, but not exclusively, focused on integrity and availability
  - For example, confidentiality of IP can be assured by interrogating fabrication process data to check that overproduction did not occur.
- TF is primarily, but not exclusively, focused on non disclosure.
  - For example, it is reasonable to assume (but impossible to prove) that cleared personnel have not subverted the fabrication process.
- Both methods are needed in order to meet DoD programmatic needs.

Overlays for DoD Microelectronics Needs

- DoD needs can be met by designing and implementing overlays on commercial processes.
- DoD needs access to a portfolio of overlays:
  - A high integrity overlay over standard commercial practice which implements a data centric independent set of checks. MQA is such an overlay.
  - An ITAR/EAR compliant overlay which ensures that information and intellectual property is not exposed to non US persons.
  - A classified overlay which ensures that classified information and intellectual property is not disclosed to unauthorized parties. TF is such an overlay.
- These overlays are related but distinct. DoD programs should have access to a portfolio of overlay options from a variety of suppliers to meet programmatic requirements.

TF vs MQA: A False Dichotomy

- Forcing a binary choice between two imperfect systems is wrong.
- MQA, as intended, is a data-centric system to assess integrity.
- TF as implemented, is a human-centric system which focuses on confidentiality.
- Both succeed or fail based on underlying systems (for example security clearance or material handling practices), and these underlying systems must fill gaps in either methodology.
- Legacy facilities with no automation are already human centric and MQA data artifacts will add little value.
- Leading edge facilities are already data-centric and forced human-centric systems will be costly and add little value.

DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited

Section II:

FINDINGS

Executive Summary: Findings

- Finding 1: DoD needs access to the commercial supply chain
- Finding 2: A risk based approach is needed
- Finding 3a: Assurance cannot be quantified
- Finding 3b: MQA offers enhanced integrity of commercial parts
- Finding 3c: The DoD approach to MQA development has gaps
- Finding 3d: RAMP is piloting MQA with very limited resources
- Finding 3e: MQA shows promise but further work is needed
- Finding 3f: MQA is at the prototype stage
- Finding 3g: Unclear how MQA is resourced
- Finding 4: Trusted Foundry offers confidentiality protection
- Finding 5: ME assurance standards have significant gaps
- Finding 6: DoD lacks adequate ME assurance governance
- Finding 7: MQA and Trust are complementary

Finding 1: The Commercial Imperative

- DoD requires access to assured microelectronics across multiple semiconductor technologies and nodes to meet system requirements and maintain warfighter advantage.
- Most DoD microelectronics components require use of commercial suppliers.
  - COTS, including FPGAs, are made by commercial suppliers, most of which have part of their supply chain overseas.
  - DMEA accreditation provides a DoD overlay to supplier's accredited commercial flow, but is not utilized by all DoD CICs.
    - GlobalFoundries received DMEA accreditation for its 12 nm process 31 Mar 2023.
    - There is no plan of record for DMEA accreditation for technologies more advanced than 12 nm.
  - USD(A&S) in partnership with the CHIPS Program Office can provide a path for assured access to SOTA and SOTP fabs.

DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited

Finding 2: Vulnerabilities and Risk Management

- The opportunity for a determined adversary to corrupt or otherwise exploit a microelectronics component varies significantly across the microelectronics lifecycle.
- The development and manufacturing lifecycle elements at highest risk for compromise are design, verification, packaging, post-silicon test activities, and configuration.
- The least vulnerable elements of the lifecycle, from conception to recycling, for SOTA microelectronics, is mask and wafer fabrication.
  - It would be extremely difficult for an adversary to alter the device or manufacturing process in a manner that would not be detected.
  - However, historical efforts have focused on securing these elements with minimal efforts to secure the most vulnerable parts of the lifecycle.
- **Where DoD has the most influence to mitigate the risk is where there is the greatest risk and where DoD has the least influence to mitigate the risk there is the least risk.**

Finding 3a: Assurance is not Quantifiable

- **Assurance cannot be measured or quantified; therefore, Microelectronics Quantifiable Assurance (MQA) is a misnomer and causes unnecessary confusion. Assurance can however be evaluated using evidence and analysis.**
- **MQA leverages MGUE and FPGA JFAC best practices and is intended as a data-centric system to independently assess integrity across the microelectronics development lifecycle.**
- **MQA has potential to be a long-term strategy for enhanced assurance in microelectronics.**
  - **It is intended to be scalable across foundries, technologies, across the full supply chain, and to improve assurance of ME components, in ways that non-automated and human-centric approaches cannot.**

Finding 3b: MQA Strengths, Weaknesses & Opportunities

- **MQA is not a complete monitoring system for all possible threats. It primarily addresses attacks on integrity and availability of the component to execute its mission when called upon to do so.**
- **MQA does not provide unique solutions to address confidentiality; existing ITAR/EAR and TF processes offer protection to address confidentiality.**
- **In the manufacturing phases, MQA is best suited for modern, highly-automated facilities, which makes it attractive for use in accessing SOTA CMOS technology.**
- **The MQA independent checks increase confidence that a DoD part created by an already good commercial process has not been compromised.**
- **The success of MQA is predicated on the willingness of domestic and international foundries to provide data for analysis.**
- **A combination of MQA and TF approaches is needed for the highest assurance applications to meet DoD programmatic needs.**

DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited

Finding 3c: The DoD approach to MQA development has gaps

- COTS is the highest volume segment of microelectronics procured for DoD programs, yet MQA as currently pursued by USD(R&E) includes FPGAs and Custom ICs but not COTS microelectronics.
- Current MQA activities focus on data products and analytics and the modernization roadmap lacks clearly defined goals of what success looks like. Additional emphasis needs to be given to a comprehensive and adequately resourced assurance strategy to include implementation:
  - What specific types of data are needed and how will they be analyzed? Who will analyze?
  - How long will the MQA process take in practice? To pilot, establish and implement?
  - How much will this process cost? What is impact to program budgets? Has DoD considered overall cost impact?
- MQA activities as part of the RAMP program are under resourced. Combined with lack of a roadmap, this seriously hampers development of the approach.

DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited

Finding 3d: RAMP is the only DoD Program developing MQA

Rapid Assured Microelectronics Prototypes (RAMP) is the DoD's most significant investment to develop and pilot MQA.

- **Primary objective of RAMP: "To develop a secure design and prototyping capability to demonstrate how the DoD can securely leverage State-Of-The-Art (SOTA) microelectronics technologies without depending on a closed security architecture fabrication process or facility."**
- **The scope of RAMP was limited to DoD CICs and the design and foundry phases of the supply chain.**
  - **At the time of this study a preliminary assessment of MQA for the design phase was complete, while MQA for manufacturing was still in progress.**
- **Two DIB design teams successfully taped out three ICs using three different Electronic Design Automation (EDA) flows and two different foundries, in an IL-4 (CUI-capable) cloud environment.**
  - **Both design teams and both foundries successfully delivered requested data to the government.**
  - **Most of the additional effort required for meeting MQA requirements was due to the pilot nature of the project, would be reduced for a subsequent design, and reduced even further with automation.**

[1] https://www.cto.mil/ramp-project/

DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited

Finding 3e: RAMP shows promise but further work is needed

- **Requested data is generally already captured as best practice, but not formatted, compiled, or shared.**
- **Data reporting was manual and varied widely, adding effort and inconsistency to data analysis.**
- **Sharing proprietary data was a major barrier and may be difficult to scale beyond the pilot demonstration without a new approach.**
- **Likelihood and impact of threats are not currently quantified – they are treated equally in terms of risk.**
- **The RAMP Phase 2 pilot *did uncover inconsistencies, undetected vulnerabilities, and gaps* in design MQA data.**
- **Further work is needed to:**
  - **Align with acquisition and sustainment programs.**
  - **Promote uniformity in data reporting, and to enable automation of data reporting and analysis.**
  - **Develop actionable remedies to risks/concerns; there could be significant impact to cost/schedule when a security threat is raised that is not in real-time.**
  - **Develop guidance on tolerable risk.**
- **The hardware assurance threat space constantly evolves, and the CIC data framework must have a process for updates to be effective**

[1] The panel was briefed by USDR&E (Matt Kay and Linton Salmon), the prime for RAMP (Microsoft), one integrated red team (Batelle, part of the RAMP program), and one independent red team (MITRE, study (supported by OUSDR&E)

Finding 3f: MQA Maturity

- MQA currently exists as a prototype stage and must continue to be developed and matured.
- RAMP demonstrated that MQA data requirements are well aligned to commercial best practices.
- RAMP has succeeded in identifying initial data needs and useful mitigation strategies, but gaps remain regarding design data capture and automation of the assessment.
- The maturity of MQA will be gradual and inconsistent across different parts of the supply chain.
- Currently, MQA development is not sufficiently resourced nor is it comprehensively structured.
- MQA is less mature than TF: using this as an excuse to fail to act is wrong.
- Barriers exist to sharing best MQA practices across the DoD which hampers scaling the approach.

Finding 3g: MQA Resources are unclear

	Govt FTE	SETA FTE	Total FTE
Pilot Programs	.75	3.2	3.75
Microelectronics Assurance Technical Execution Area	81	134	215
Policy, Standards and Guidance:	0	1.75	1.75

Includes RAMP & SHIP

Includes all T&AM microelectronics assurance work funded by R&E

Includes efforts for MQA and Microelectronics Assurance Framework.

Based on the information provided by USD(R&E) it is not possible to ascertain the sum total of resources dedicated to MQA development.

DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited

Finding 4: Trusted Foundry

- TF refers to the process used by DMEA to provide access to classified or export-controlled parts through a select supplier set.
  - TF is a system focusing primarily on *confidentiality*. It assumes but does not verify that commercial best practices assure *integrity*.
  - Trusted flows protect access to classified or otherwise sensitive information in ME during design, mask and wafer manufacturing, and packaging from unauthorized personnel.
  - Currently, TF is only available at SOTP and Legacy nodes.
- Legacy Trusted models that rely on human-centric controls are incompatible with SOTA ME fabrication.
- Leading edge facilities are highly automated and data-centric. Commercial best practices provide the baseline of integrity and confidentiality controls that can support enhancements for DoD's requirements.
- Commercial best practices overlayed with V&V of integrity and/or confidentiality control plans enable export control and classified flows.

DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited

Finding 5: Standards

- **Congressional intent to have microelectronics standards deployed did not meet original deadline and is still ongoing.**
- **No standard currently exists for microelectronics assurance BUT there are many standards that can inform microelectronics assurance, including defining best practices. For example, ISO 26262 Automotive, SAE 21434 and ISO/IEC 15408 Common Criteria.**
- **Commercial fab standards do not exist (fab line operations are not standardized), but best practices employed by SOTA fabs DO exist and largely address confidentiality and integrity. <u>SOTA fabs employ the utmost protections for confidentiality of IP. Malicious attackers would find almost everything else a softer target.</u>**
- **Industry is heavily invested in standards development and compliance.**
- **Combination of Standards and Guidance are needed to best effect future assurance.**
- **Current DoD approaches on methodologies and standards conflate the creation of a microelectronics part and its use in a DoD system. Different standards are needed for the creation of a part and its use in a DoD system.**

DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited

Finding 6: DoD Lacks Adequate ME Assurance Capability

- MQA is focused on component assurance but the DoD acquires systems, not components. No current guidance provides sufficient context and information to make well informed risk-based decision on the impact of component assurance to system resilience.
- DoD lacks access to necessary assurance expertise.
- There exists a general lack of awareness of JFAC Hardware Assurance Labs and their capabilities to support DoD programs.
- JFAC is not adequately resourced or structured to provide programmatic support of component risk assessment.
- The national security community does not currently have the tools, standards, techniques and workforce to comprehensively address the needs of SOTA.

DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited

Finding 7: MQA and TF are complementary

- Trust delivers confidentiality options to the DoD while MQA delivers integrity options for using the commercial supply chain.
- The human centric approach of TF leaves it vulnerable to integrity and confidentiality violations. This shortcoming can be remedied by requiring MQA on the underlying commercial process.
- The data centric approach of MQA cannot address the policy requirements for ITAR/EAR and classified information which limit exposure based on nationality and/or clearance. This shortcoming can be mitigated by using TF or an ITAR overlay on top of MQA when classified information or ITAR/export control or requirements exist.
- It is not either/or.

Section III:

ANALYSIS

Executive Summary: Analysis

- The DoD must adopt a risk based approach.
- The riskiest stages of the ME lifecycle are design, packaging, post-silicon validation, packaging, configuration and programming. We need to invest more here. MQA addresses this (although not completely and not exclusively)
- The least risky stages are mask and wafer fabrication. We need to invest less here. TF addresses this (although not completely and not exclusively)
- Not all DoD programs are the same. Their requirements vary. Some programs only need access to high quality commercial flows. Others may have ITAR/EAR restrictions. Yet others may include classified information that requires protection. All need access to a high quality, independently checked design and manufacturing process.
- These different needs can be accommodated by creating a portfolio of options for programs implemented through a set of standardized and independently verifiable overlays over commercial processes.

Risk is not only about making mistakes, but also failing to act and failing to evolve.

ANALYSIS:

RISK AND INFLUENCE

The Nature of Risk and Microelectronics

- Risk is a function of the likelihood of an event happening and the magnitude of the loss should the event occur.
- The likelihood of the event occurring, for example, an adversary successfully affecting the confidentiality, integrity and availability of a part is a function of how capable the adversary is, how valuable the attack would be to them, how many exploitable vulnerabilities does the part or the process have and how long does the adversary have to exploit them as well as the cost to them if discovered.
- The ability of DoD to mitigate ME risk is a function of how much control the DoD has on the setting requirements of a program, adequate program control and DIB performance.
- Recognizing that eliminating risk completely is impossible how to we best define how much risk we should tolerate in our microelectronics?
- We would like to limit the risk we assume to be as low as reasonably practicable.

> "[Risk is] A probability or threat of damage, injury, loss, or any other negative occurrence that is caused by external or internal vulnerabilities, and that may be avoided through preemptive action."

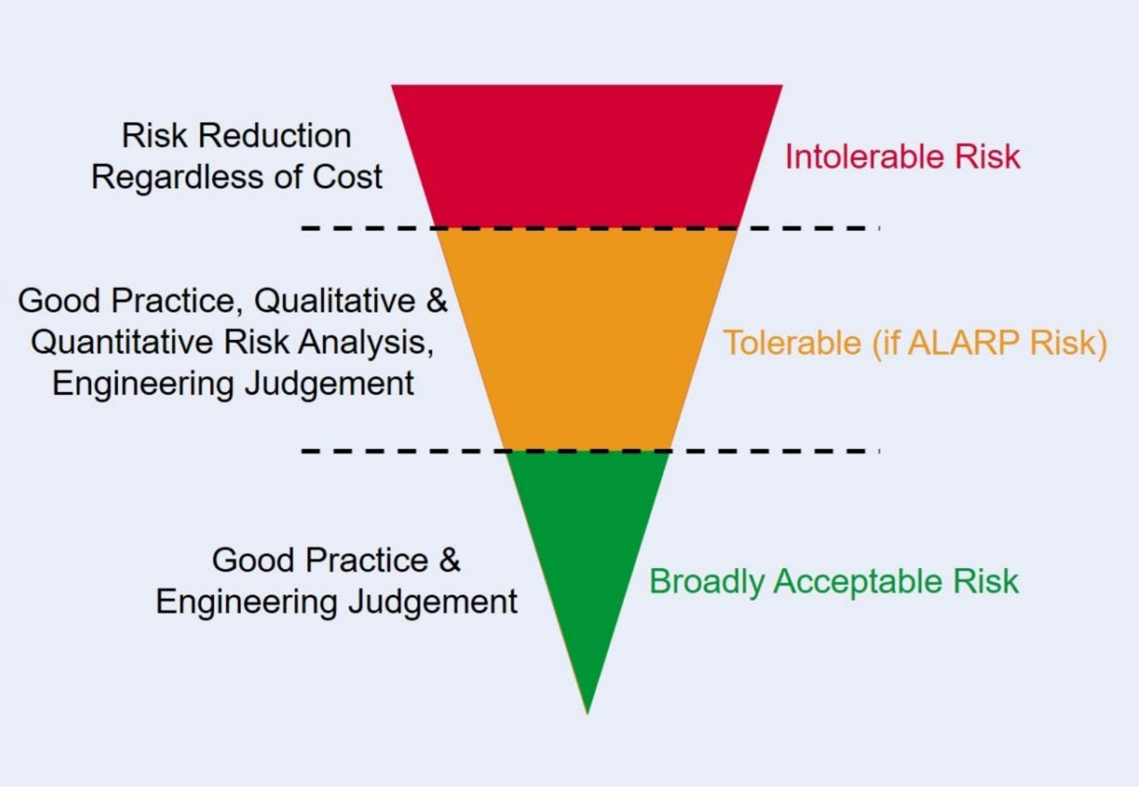
How Much Risk to Assume: ALARP

“ALARP is short for "as low as reasonably practicable". Reasonably practicable involves weighing a risk against the trouble, time and money needed to control it. Thus, ALARP describes the level to which we expect to see workplace risks controlled.”

UK Health and Safety Executive

In the UK MOD the Duty Holder Chain of Command are the only people who can accept risk and declare that a risk is Tolerable and ALARP.

Most of DoD programs fall in the bottom two categories. There is no known DoD program that has fabbed chips with the mindset that risk reduction regardless of cost is a priority.


Risk Reduction Regardless of Cost
Intolerable Risk
Good Practice, Qualitative & Quantitative Risk Analysis, Engineering Judgement
Tolerable (if ALARP Risk)
Good Practice & Engineering Judgement
Broadly Acceptable Risk

DoD Risk Across the Microelectronics Lifecycle

- Assessment of consequence and likelihood for Integrity and Confidentiality
  - Based on currently available mitigations

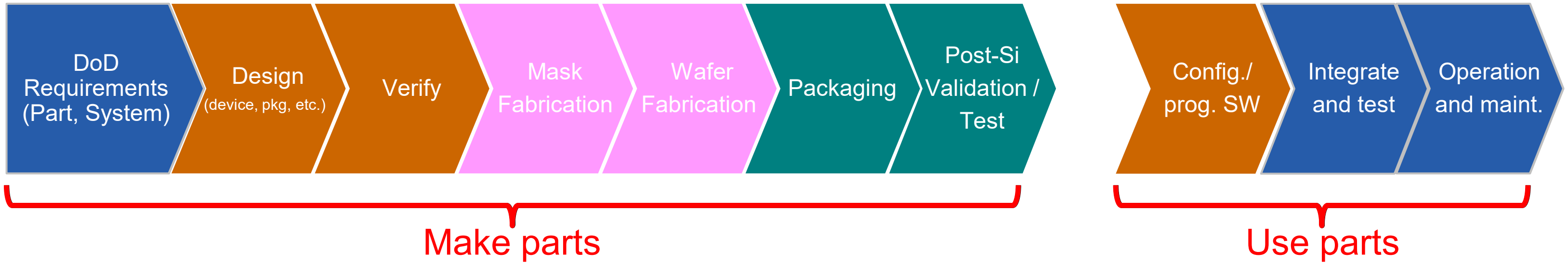
	Make parts							Use parts		
	DoD Requirements (Part, System)	Design (device, pkg, etc.)	Verify	Mask Fabrication	Wafer Fabrication	Packaging	Post-Si Validation / Test	Config./ prog. SW	Integrate and test	Operation and maint.
PRODUCT INTEGRITY (alteration)										
CONSEQUENCE	HIGH	HIGH	HIGH	HIGH	HIGH	HIGH	HIGH	HIGH	HIGH	HIGH
LIKELIHOOD	PROGRAM	HIGH	MED	LOW	LOW	HIGH	HIGH	HIGH	PROGRAM	PROGRAM
RISK LEVEL	*PROGRAM*	*HIGH*	*MED-HI*	*MED-LO*	*MED-LO*	*HIGH*	*HIGH*	*HIGH*	*PROGRAM*	*PROGRAM*
CONFIDENTIALITY										
CONSEQUENCE	MED-HI	HIGH	HIGH	MED	MED	MED-HI	HIGH	HIGH	PROGRAM	PROGRAM
LIKELIHOOD	PROGRAM	PROGRAM	PROGRAM	LOW	LOW	MED-HI	MED-HI	PROGRAM	PROGRAM	PROGRAM
RISK LEVEL	*PROGRAM*	*PROGRAM*	*PROGRAM*	*LOW*	*LOW*	*MED-HI*	*MED-HI*	*PROGRAM*	*PROGRAM*	*PROGRAM*

- **'PROGRAM' = DoD Programmatic decisions drive likelihood rather than anything inherent to that part of the lifecycle**

DoD Influence Across the Microelectronics Lifecycle

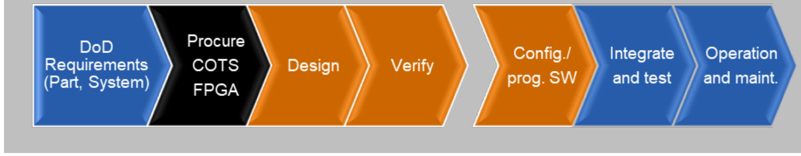
Current Status: stages of the ME lifecycle that the DoD can manage risk based on current influence

Custom Integrated Circuit (CIC)

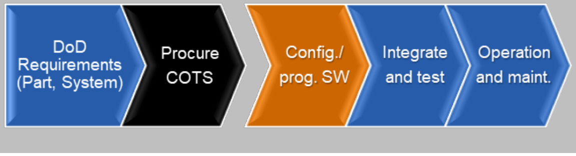


- 🟦 **These phases are controlled by the DoD program; DoD influence over requirements is HIGH**
- 🟧 **Tasks commonly performed by DIB performer; some commercial performers. DoD influence remains generally high**
- 🟩 **Tasks commonly performed by commercial entities (esp. SOTA), but DoD influence via DIB performers and ability to overlay DoD requirements**
- 🟪 **Tasks performed by commercial entities, with limited ability to overlay DoD requirements or flows (e.g., MQA, Trust)**
- ⬛ **Commercial components; developed in the absence of DoD requirements**

FPGA



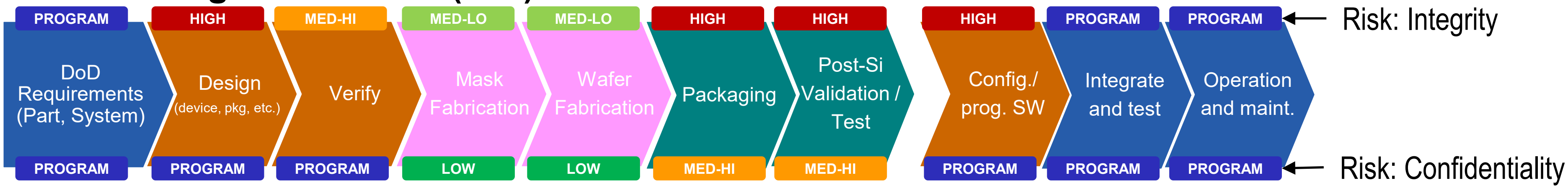
COTS in DoD Systems



DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited

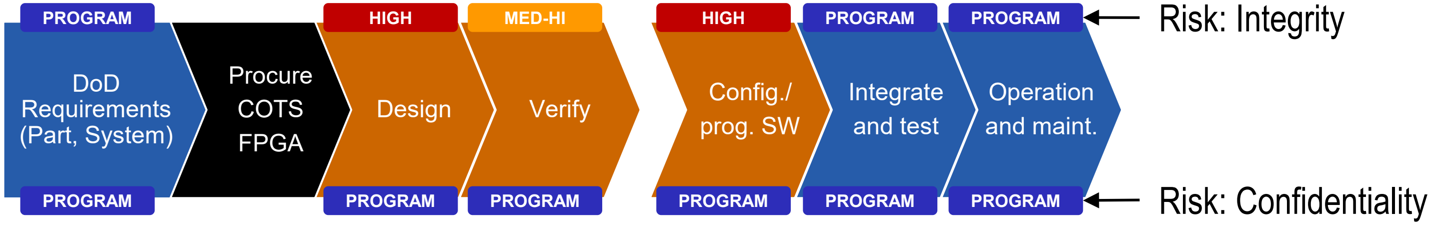
DoD Influence and Risk Across ME Lifecycle

Custom Integrated Circuit (CIC)



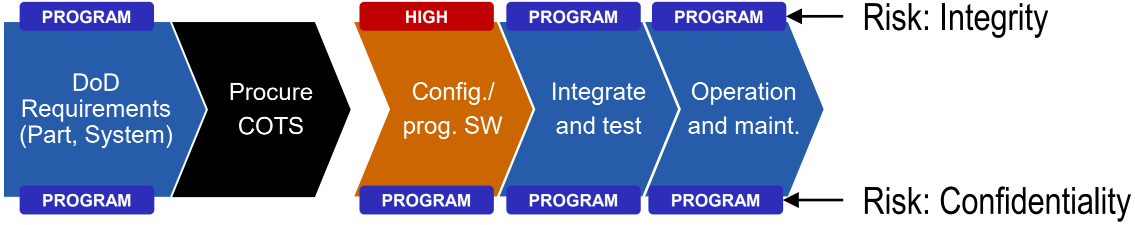
	DoD Requirements (Part, System)	Design (device, pkg, etc.)	Verify	Mask Fabrication	Wafer Fabrication	Packaging	Post-Si Validation / Test	Config./ prog. SW	Integrate and test	Operation and maint.
Risk: Integrity	PROGRAM	HIGH	MED-HI	MED-LO	MED-LO	HIGH	HIGH	HIGH	PROGRAM	PROGRAM
Risk: Confidentiality	PROGRAM	PROGRAM	PROGRAM	LOW	LOW	MED-HI	MED-HI	PROGRAM	PROGRAM	PROGRAM

Semi-Custom (FPGA)



	DoD Requirements (Part, System)	Procure COTS FPGA	Design	Verify	Config./ prog. SW	Integrate and test	Operation and maint.
Risk: Integrity	PROGRAM		HIGH	MED-HI	HIGH	PROGRAM	PROGRAM
Risk: Confidentiality	PROGRAM		PROGRAM	PROGRAM	PROGRAM	PROGRAM	PROGRAM

COTS for DoD Systems



	DoD Requirements (Part, System)	Procure COTS	Config./ prog. SW	Integrate and test	Operation and maint.
Risk: Integrity	PROGRAM		HIGH	PROGRAM	PROGRAM
Risk: Confidentiality	PROGRAM		PROGRAM	PROGRAM	PROGRAM

- 🟦 **DoD program control: HIGH DoD influence**
- 🟧 **DIB tasks: generally HIGH DoD influence**
- 🟩 **Commercial tasks: DoD influence via DIB**
- 🟪 **Commercial tasks: limited DoD influence**
- ⬛ **Commercial components: no DoD influence**

Risk and DoD influence are both low for SOTA mask and wafer fab, contrary to common belief
*** Investment in heightening assurance for mask and wafer fab should NOT be the priority ***

ANALYSIS:

MGUE EXPERIENCE LED TO MQA

DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited

Military GPS User Equipment (MGUE) Next Generation ASIC

- **GPS signals are easy to jam and spoof.** The M-Code signal is a more powerful, encrypted signal to help military users overcome jamming and protect against false GPS signals being used to spoof users by misdirecting them.
- The goal of MGUE Inc 2 is to develop, integrate, and produce M-Code capable, GPS receivers for the service requirements specified in the Joint Requirements Oversight Council (JROC) approved MGUE Inc 2 Capability Development Document (CDD).
- The MGUE Inc 2 acquisition strategy includes award of up to three development contracts to develop a low size & power Minature Serial Interface (MSI) form factor to include a next generation application-specific integrated circuit (ASIC). The MSI receiver card must meet low size, weight and power (SWaP) constraints. The ASIC within, however, must be built to meet the needs of not only this form factor but all platforms the contractors may use it in.
- MGUE asserted that ASIC designs that do not contain military specific features, such that features cannot be revealed until post-manufacture provisioning, should not trigger ITAR requirements.
- The first "technology-enhanced" ITAR removed defense-related technical data from the design enabling programs with greater access and led directly to the development of the MQA approach.

MGUE Experience

- The technology needed to meet MGUE performance requirements were not available via standard DoD access methods (i.e., were not available via DMEA accredited or ITAR compliant sources)[1]
  - No viable alternative technical solutions (architectures, technologies, requirements relief) were identified in program and vendor studies.
  - MGUE Program Manager indicated release of Inc 2 RFP was dependent on clear path to manufacturability, requiring solution to both Trust and ITAR issues.
- DoDI 5200.44 requires use of DMEA accredited facilities and flows for DoD custom integrated circuits.
  - Requests for relief from requirement were denied by OSD(AT&L).
  - In response, MGUE developed an analysis to substantiate their claims that they could apply mitigations to access necessary technology in a manner commensurate with program security requirements.
    - Approach was coordinated broadly (e.g., JFAC, DARPA, Sandia National Labs, OSD).
    - More than 80% overlap between MGUE solution and MQA CIC LoA-1 draft guidance.
    - Approach was approved by USD (AT&L) and cited as a pilot approach for DoD microelectronics access.
    - This success enabled award of efforts through MGUE ASIC Preliminary Design Review (PDR.)
- ITAR controls for DoD ASICS do not clearly address modern System on Chip (SoC) architectures, creating another barrier to access.
  - MGUE worked closely with Defense Technology Security Administration (DTSA) and OSD(R&E) to develop clarification to ITAR, published 2019.
  - MGUE vendors successfully obtained Commodity Jurisdictions from Dept of State, ruling that MGUE ASICs are not ITAR *as manufactured.*
    - This success enabled award of MGUE Inc 2 contracts (RFP released Dec 2019)
- <u>**Enabling access to technology unavailable in Trusted and ITAR ecosystem took more than 2 years.**</u>

[1] GF 14 nm became ITAR compliant in 2020 and DMEA accredited Mar 2023

MGUE Lessons Learned

- MGUE is in the design and verification phase of their ASIC development
- Success:
  - RTL and verification assessment artifacts place relatively low burden on development.
- Challenges:
  - Third party intellectual property (3PIP) licensing and data rights challenges can derail assurance requirements.
    - MGUE required vendors to provide all design information, and required the performers to share this information with JFAC.
    - Due to NDA and data rights issues, design databases delivered are missing critical IPs limiting the ability to rebuild and independently verify the design.
    - Ecosystem evolution – DIB and supplier ecosystem changes further complicate contracts and data rights.
  - DoD needs consistent and broad access to SOTA EDA tools.
  - Data sharing requirements and mechanisms must be improved.
    - CDRLs should include acceptance criteria.
    - Design data not currently standardized.
    - Design portability is not considered.

MGUE Execution Enabled Access to Commercial Foundry hence demonstrating that DoD requirements can be met by commercial foundries.

ANALYSIS:

BASIS FOR CONFIDENCE: MQA

The RAMP MQA Pilot Effort

IS…

- An effort to "pipeclean" MQA.
  - Seek and expect correction to CIC standard.
  - An interactive partnership with RAMP participants.
- Leverages data already created in the commercial flow.
- Exercise of version 3.0 of the CIC standard.
- Limited to LoA-1 level of assurance.
- MQA from design through wafer fab/ship.
- Three representative designs (digital, chiplet, M/S).
- An effort to develop detailed feedback on V3.0.
- An evaluation of LoA-1 threats, associated mitigations and data requirements.
- Evaluation of data and data format for data provided during design and wafer fab.

IS NOT…

- The definitive effort to define MQA.
  - Use of the "final" version of the CIC standard.
  - A mandate to RAMP participants.
- A research project to generate new data artifacts.
- Pilots of FPGA or COTS draft standards.
- Not reflective of LoA-2 or LoA-3 requirements.
- MQA for packaging.
- Representative of ALL possible DoD designs.
- An effort to define MQA strategy or policy.
- An evaluation of all possible threats or mitigations for DoD microelectronics.
- Definition of the most efficient ways to collect and evaluate MQA data.
- Analysis of remaining risks (JFAC task).

DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited

RAMP Pilot Overview

- Three DoD design chosen for pilots.
  - BAE space microprocessor (Digital).
  - BAE N-Path (Mixed Signal).
  - Raytheon digital transceiver (Chiplet).
- Two major flows used to fabricate pilot designs.
  - Intel 16 (2).
  - GlobalFoundries 12LP (1).
- Major EDA companies.
  - Ansys, Cadence, ClioSoft, Siemens EDA, Synopsys, Cycuity.
  - 2 integrated flows demonstrated (BAE and Raytheon).
- Two major purposes for the RAMP pilots.
  - Exercise Microsoft commercial cloud design environment for DoD ASICs.
  - Pipeclean version 3.0 draft of the CIC MQA standard.
- Pilot schedule:
  - November, 2021: Design start.
  - December, 2022: Design tapeout to wafer fab (MQA data evaluation for design nearing completion).
  - May, 2023: Completion of wafer fabrication runs (MQA data evaluation for manufacturing is ongoing).
  - August, 2023: Completion of RAMP Phase 2.

RAMP Pilot Results: Successes

- LoA-1 minimum requirements expected to be met using commercially available data.
  - All threats addressed by mitigations and data.
  - Confirmation of suitability for LoA-1 applications pending risk analysis effort by JFAC.
- LoA-1 requirements are well aligned to commercial processes.
  - All data (except country of origin) was confirmed to be taken during the design and manufacturing processes.
  - Exceptions:
    - Assurance focused evaluation of 3PIP is not typical and may require additional effort by CIC design team.
    - Manufacturing mitigations leverage existing data, but capture and reporting required extra effort and standardization.
- RAMP successfully utilized cloud infrastructure to navigate delivery of large amounts of data to the government and its reviewers.
  - Navy ATO expected FY24 Q2, will utilize MOU/MOA for access by other services.
  - Authority to Operate (ATO) permission is required *by each DoD entity using it*.
- Expected schedule in the flow for data delivery was refined.
  - Initial expectations for MQA data delivery had to be modified to better match standard design flows.
  - CIC development milestones not always initially well aligned to acquisition milestones (e.g., PDR, CDR).
    - Further changes expected for DIB design teams utilizing an agile development method

DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited

RAMP Pilot Results: Needs Improvement

- Data delivery format and level of detail needs to be standardized in greater detail.
  - Delivery format varied by performer.
  - Delivery format needs to address needs of provider and needs of the reviewer.
  - RAMP will generate a lessons learned document; JFAC will integrate into MQA Best Practices Guide currently being developed.
- Standardization improves usability and performance by performers (DIB, commercial) and independent reviewers.
  - Supports performers by providing clear expectations of deliveries; minimizing interpretations of requirements.
  - Supports evaluators by enabling use of work instructions; minimizing variation in interpreting data.
  - Enables eventual automation for delivery and evaluation.
  - RAMP is addressing this via: automation of data formatting, searchability, streamlining of data acceptance screening and analysis.
  - JFAC/Navy effort toward verification work instructions.
- Better communication of MQA goals to the DIB will be needed.
  - This is not just prime contractors and foundries – alignment on goals was essential to enabling data sharing and support from EDA tool vendors and 3PIP vendors.
  - Submission of the data package should be viewed as a requirement.
  - The pass/fail perspective should be replaced with the perspective that the data will be used for residual risk analysis by the program office.

RAMP Pilot Results: MQA Data Analysis

- Data rights and data sharing were a major challenge and require a more holistic approach.
  - 3PIP challenges were limited in RAMP, but deliveries remained on a per-name basis due to licensing restrictions.
  - Issue is not limited to 3PIP; some EDA vendors require NDAs to view tool outputs.
    - EDA tool outputs are foundational to verification and validation activities.
- The volume of data requested, let alone available, makes analysis daunting.
  - Finding small needles in large haystacks; guided by goal to address the listed integrity and confidentiality threats.
    - Planned improvement through work instructions to guide evaluators through data analysis.
  - PDR was the longest review time, as it was the first pass for all participants.
    - Processes put in place at DIB and foundries that sped up provision/analysis of each subsequent MQA data drop.
  - There is an opportunity to leverage Machine Learning to assist in analysis (example: reticle locations).
- Correlation between different data requirement items promises to provide great insights.
  - Current method of review emphasizes evaluation of data in a single mitigation or data requirement.
  - Correlation is very difficult to establish manually – need to develop automation and tools.
  - An example is correlating IP verification files with the chip floorplan/IP list.

ANALYSIS:

OVERLAYS

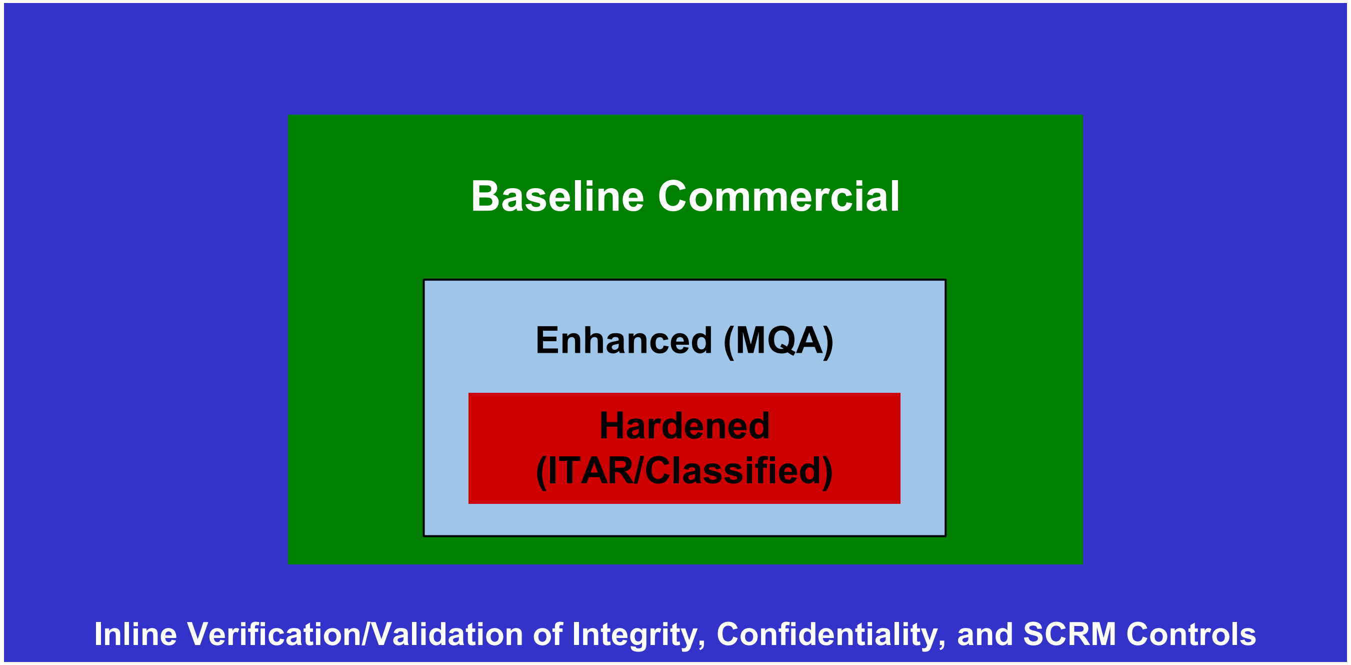
Not all DoD programs are created equal

- DoD programs have varied requirements hence ME assurance cannot be one size fits all. For example nuclear weapons and office equipment occupy very different ends of mission impact.
- Program needs fall into four different categories:
  a. Procured from a reputable commercial ME supplier.
  b. Procured from a reputable commercial ME supplier implementing an MQA overlay for higher integrity and confidentiality.
  c. Procured from a reputable commercial ME supplier implementing an MQA overlay for higher integrity and confidentiality plus an ITAR/EAR overlay to preclude exports as defined in ITAR 120.17
  d. Procured from a reputable commercial ME supplier implementing an MQA overlay for higher integrity and confidentiality plus a classified overlay to ensure non disclosure of classified information to unauthorized persons.

DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited

Overlays

- An overlay is a set of additional steps and processes overlaid over a commercial flow designed to ensure additional ME assurance to meet DoD program requirements.
- TF is an example of such an overlay over commercial process.
- Overlays support mix-and-match requirements.


Baseline Commercial
Enhanced (MQA)
Hardened (ITAR/Classified)
Inline Verification/Validation of Integrity, Confidentiality, and SCRM Controls

DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited

Overlay design is not trivial

- Overlay design, as the MQA RAMP pilot demonstrates, is far from trivial and requires dedicated development, piloting, standardization and deployment. For example:
  - Classified overlays are a data handling matter and the solution does not require separate fabrication lines.
  - ITAR/EAR overlays are not the same as Classified overlays:
    - Classified exceeds the security requirements of an ITAR flow.
    - Commercial manufacturers must have an in house export compliance program and office to manage non classification related aspects of ITAR.
- <u>There are wildly varying estimates for the cost of implementing a classified overlay, ranging from $200M to $5B. These estimates are not credible without analysis and justification.</u>
- We need to standardize only on what is <u>necessary and sufficient</u> to achieve the assurance level required.
- Expertise to determine the required overlays exist within government agencies as well as the commercial sector.

Notional Overlays

Assurance = f (Confidentiality + Integrity + Availability*)

***This review is focused only on Confidentiality and Integrity for SOTA ME**

Confidentiality Notional Flows

- **Zone 3: Commercial best practices**
  - Ex.: Commercial personnel vetting and insider threat training
  - Ex.: Commercial industry IT and cybersecurity practices
- **Zone 2:** A commercial process that ensures sensitive but unclassified (ex. CUI, export controlled) information and IP is protected per regulations/policy
  - Ex.: Wafer Scrap Procedure
  - Ex.: Data Segregation and Access control
  - Ex.: USP only for export-controlled information
- **Zone 1:** A commercial-based process that ensures classified information is protected per regulations/policy
  - Ex.: Design occurs in/on a classified environment/network
  - Ex.: Cleared personnel oversight in Fab of wafer and mask handling
  - Ex.: Packaging facility and tools access within a protected space (SCIF)

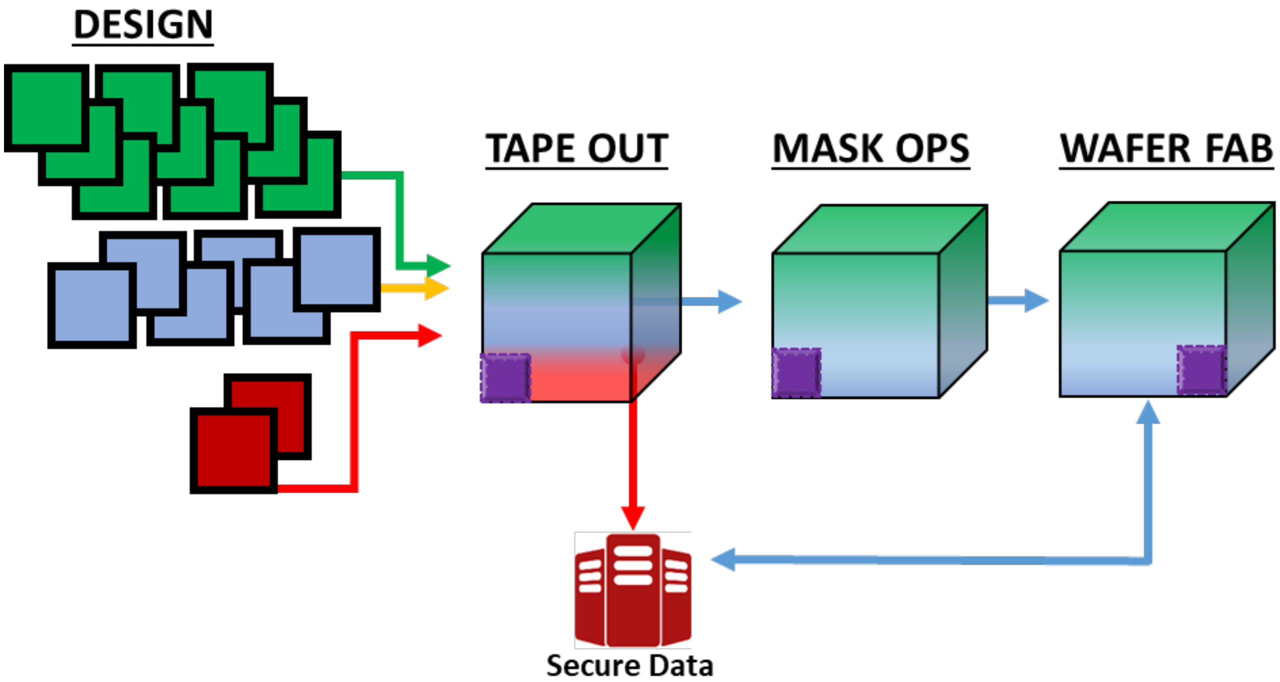
Integrity Notional Levels

- **Level C: Commercial best practices** for commercial & commercial-developed custom products
  - Ex.: Enterprise Laptops
  - Ex.: Commercially available FPGAs
  - Ex.: Commercially developed ASICs
  - Ex.: baseline extensive commercial testing to ensure commercial product viability.
- **Level B:** Leverage and Verify/Validate evidence-based commercial best practices to establish additional **assurance** of device integrity
  - Ex.: Design 3PIP Integrity Verification/Validation at Design
  - Ex.: Wafer Test Verification/Validation
- **Level A:** Extensive verification and validation of integrity by DIB and/or USG is performed
  - Ex.: pre-fab independent verification of pre-silicon design by service identified subject matter experts
  - Ex.: post-fab JFAC physical evaluation of device

DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited

Overlays on commercial process

MICROELECTRONICS DESIGN AND FABRICATION



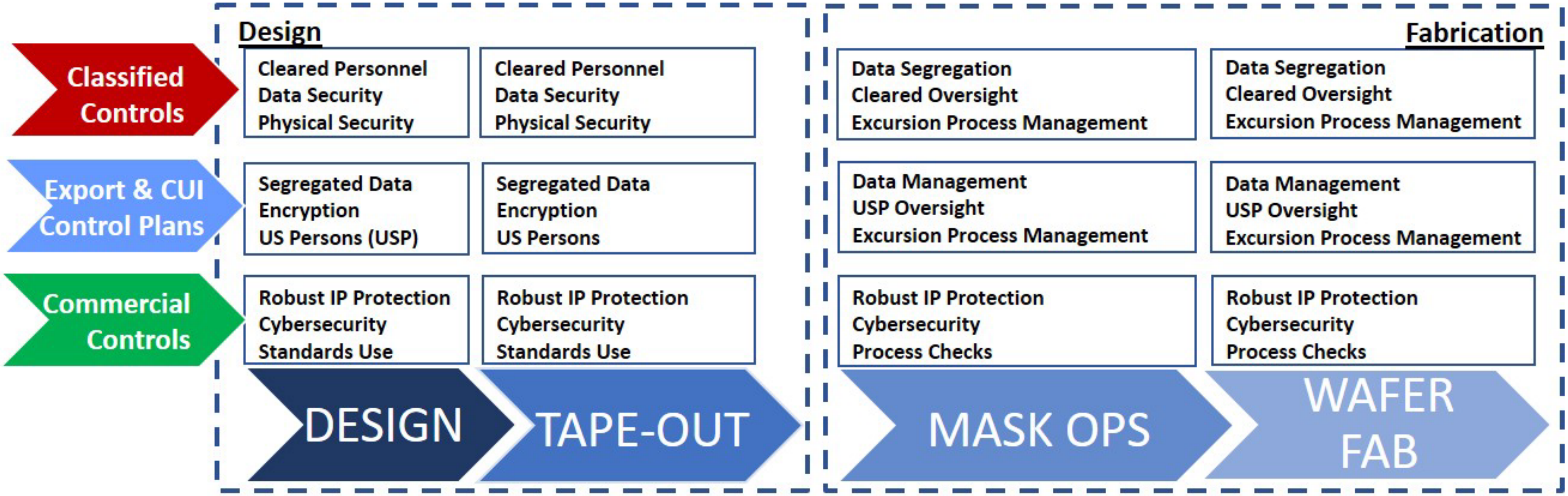
Confidentiality Controls:

UNCLASSIFIED	ZONE 3: Commercial Baseline Protection
SENSITIVE	ZONE 2: + Enhanced Protections
CLASSIFIED	ZONE 3: + Hardened Protections
OVERSIGHT	+ USP and/or Cleared Persons

Control Plans Overlay Commercial SOTA Flows

The Design phase of the flow must be protected to ensure confidentiality. The Fabrication flows only require access controls and oversight to address confidentiality.

*** Investment in heightening physical security for mask and wafer fab should NOT be the priority ***



	Design		Fabrication	
	DESIGN	TAPE-OUT	MASK OPS	WAFER FAB
Classified Controls	Cleared Personnel Data Security Physical Security	Cleared Personnel Data Security Physical Security	Data Segregation Cleared Oversight Excursion Process Management	Data Segregation Cleared Oversight Excursion Process Management
Export & CUI Control Plans	Segregated Data Encryption US Persons (USP)	Segregated Data Encryption US Persons	Data Management USP Oversight Excursion Process Management	Data Management USP Oversight Excursion Process Management
Commercial Controls	Robust IP Protection Cybersecurity Standards Use	Robust IP Protection Cybersecurity Standards Use	Robust IP Protection Cybersecurity Process Checks	Robust IP Protection Cybersecurity Process Checks

Overlays are commercial product offerings

- The definition and use of overlays allows commercial suppliers to choose to offer them as products or services.
- Each supplier will determine whether to offer the product or not depending on their business model. <u>The government must develop and use practices that are viable for the industrial base.</u>
- By standardizing the overlay requirements, the DoD can:
  - Encourage the creation of a stable marketplace of commercial suppliers willing to offer the product to the government.
  - Create a diverse supplier base offering the government multiple, cost effective options to meet program requirements.
  - Access high assurance microelectronics from geographically diverse allies (Europe, Japan, Taiwan for example) in addition to domestic suppliers.

DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited

Trust but Verify

- The TF overlays are an effective way to access the commercial supply chain because they augment the already highly controlled manufacturing process with an independent, highly qualified group of assessors that work side by side with the supplier to ensure and guide compliance.
- All three proposed overlays should be similarly augmented by an independent, highly qualified group of assessors.
- This independence ensures not only compliance but over time improves overall confidence in the assurance of the components by evolving our defense in depth and other measures.
- TF has been successfully demonstrating the feasibility of independent checks for many years.

ANALYSIS:

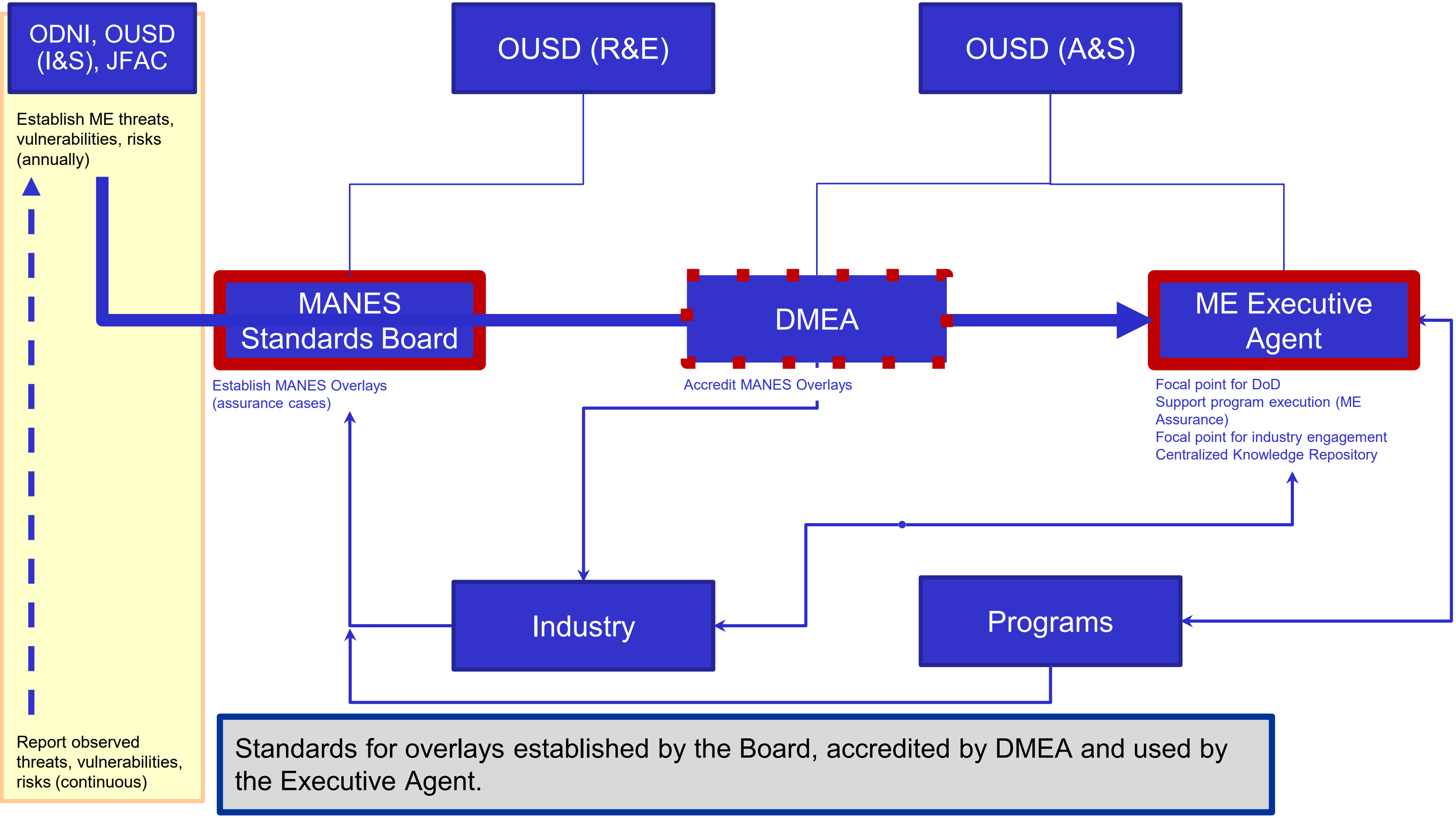
GOVERNANCE

DoD ME Assurance Governance has Gaps

- National security needs for ME Assurance span the DoD, the Intelligence Community, the DoE, the DoC and a host of other Departments and Agencies.
- The Interagency process is not as effective as it needs to be given the complexity and importance of the issue.
- The governance process has significant gaps that are contributing to suboptimal outcomes for national security.
- In particular:
  - There is no ME Assurance Executive Agent (EA) to connect DoD programs with the supply of suitable commercially sourced parts.
  - There is no group with a singular focus on creating, piloting and deploying ME Assurance standards across the national security community.
- These gaps can be filled by creating a ME Assurance EA and a ME Assurance Standards Board.

DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited

ME Assurance Governance: Notional Org Chart



ODNI, OUSD (I&S), JFAC

Establish ME threats, vulnerabilities, risks (annually)

Report observed threats, vulnerabilities, risks (continuous)

OUSD (R&E)

OUSD (A&S)

MANES Standards Board

Establish MANES Overlays (assurance cases)

DMEA

Accredit MANES Overlays

ME Executive Agent

Focal point for DoD
Support program execution (ME Assurance)
Focal point for industry engagement
Centralized Knowledge Repository

Industry

Programs

Standards for overlays established by the Board, accredited by DMEA and used by the Executive Agent.

ME Assurance Governance: Notional Roles/Responsibilities

R Responsible (does the work)	C Consulted
A Accountable (the buck stops here)	I Informed

DoD Programs (USE)	ME Developers (MAKE)	Task	MANES Standards Board primary focus MAKE	OUSD(R&E)	PD ME	OUSD(A&S)	DLA	DSPO	DMEA	OUSD(I&S)	IC (ODNI, ...)	Services	JFAC	ME Executive Agent primary focus USE	DoD Program Office	DoD Prime	DIB Performers	Commercial Industry
X		Develops and executes strategy for DoD Microelectronics		C	A, R	C	I	I	I	C	C	I	I	C	I	I	I	I
X		Writes ME Assurance policy (i.e., DoDI 5200.xx)		A, R	C	C	I	C	I	C	I	C	C,I	C	I	I	I	I
X		Develops, publishes and maintains "Program Guidance for ME Assurance"	C	A, R	C	C	I	C	C	C	C	C	C	C	I	C	C	I
X		Establish and update ME threats, vulnerabilities, and risks (annual, trigger)	C							R	A, R	C	R	C				
X		Continuous communication of ME threats, vulnerabilities, and risks		I	I	I	I	I	I	I	I	I	I	R,A	I	I	I	I
X	X	Reporting of observed ME threats, vulnerabilities, and risks		R	R	R	R	R	R	R	R	R	R	A	R	R	R	R
X	X	Develops, publishes and maintains MANES Overlays (assurance cases) for COTS, FPGA, CIC	R	A	C	C	C	C	C	C	C	C	C	C		C,I	C,I	C,I
X	X	Evaluates and accredits vendors for MANES Overlays							R,A					C				
X	X	Develop and execute strategy for adoption of MANES Overlays	C	A,R	C	R	C	C	C		C	C	C	R	C	C	C	C
X		Establishes and maintains Centralized Knowledge Repository for ME				A			C		C	C	C	R	C	C	C	C
X	X	Serve as focal point for engagement with interagency and SC industry				A								R				
X		Oversight for acquisition program use of ME Guidance (program, MANES Cases)										R	R	A, R	R			
X		Program-specific management of ME Assurance risks							C				C	C	A,R	R	R	
X		Stockpile assured COTS			C	C	A, R		C			C		C				

DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited

Integrity - Service - Excellence

ANALYSIS:

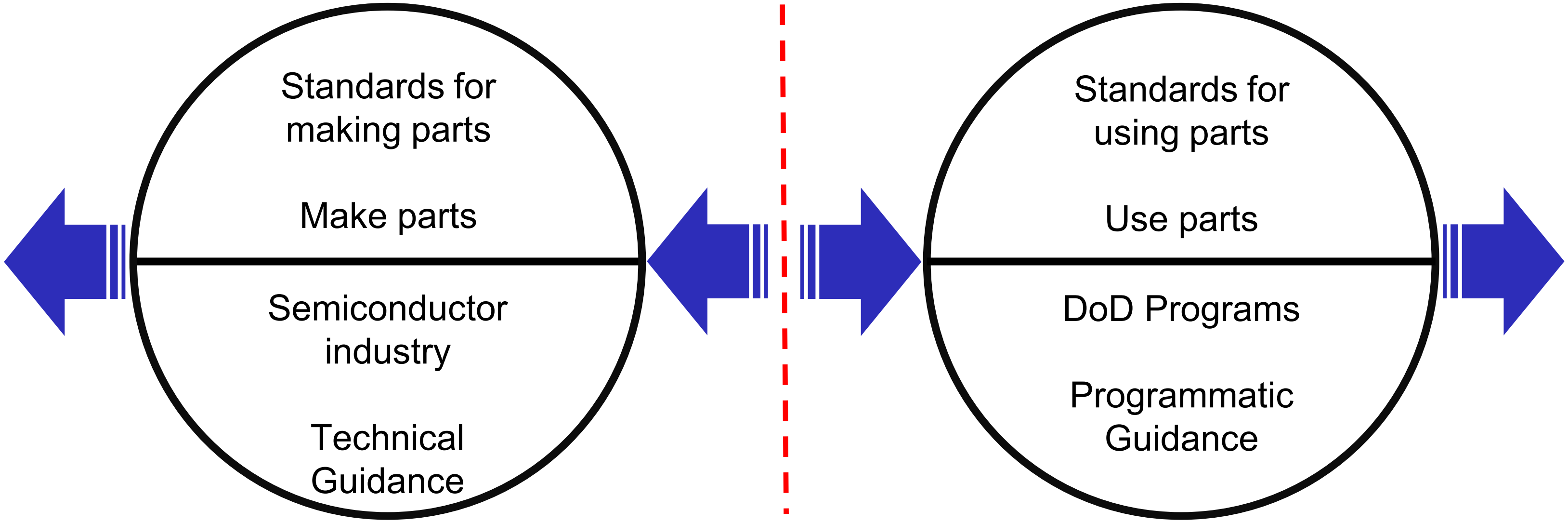
STANDARDS

The role of standards in ME Assurance

- Standards enable a consistent, systematic and repeatable way of achieving assurance in commercially developed ME.
- However, we must be clear about what can be and what cannot be standardized.
- Each manufacturer uses a different, proprietary and highly guarded process for making their products. This part cannot be standardized.
- However, we can implement a standardized, independent verification regime that is based on querying data created during the manufacturing process. We can also standardize what overlays need to implement.
- Standards should be minimally prescriptive and maximally normative, that is minimize prescribing how they should be implemented while maximizing describing what outcomes are desired by their application.

An Integrated ME Assurance Standards Framework

- Standards must integrate product with programmatic considerations to maximize DoD access to best available ME.
  - Overlay standards contain technical guidance for developing, manufacturing, procuring and validating components that will eventually be deployed in DoD systems.
  - Programmatic guidance focuses on enabling program-specific, risk-based decision making to manage microelectronics assurance risks in the context of their systems.
  - Favor guidance over prescription to the greatest extent possible.



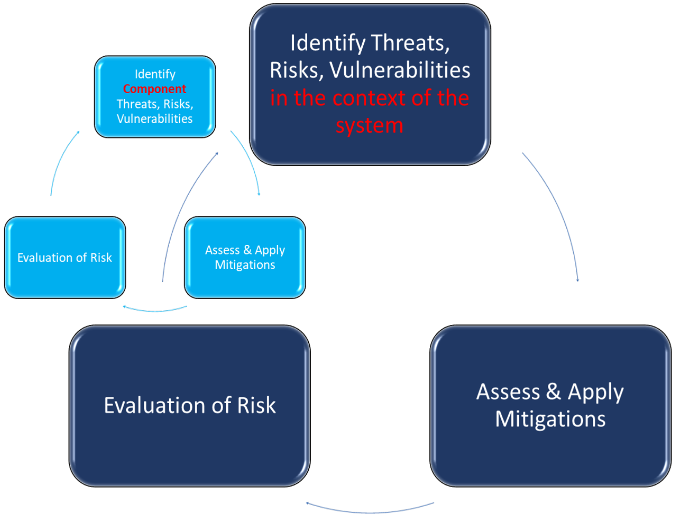
DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited

Make vs. Use Standards

Two distinct threat models are utilized: MAKE and USE

MAKE – TECHNICAL GUIDANCE - OVERLAYS

- What is the risk associated with a component doing what is should and nothing else?
- What is the risk associated unauthorized access to design or devices?
- ME Lifecycle Elements: requirements through configuration.



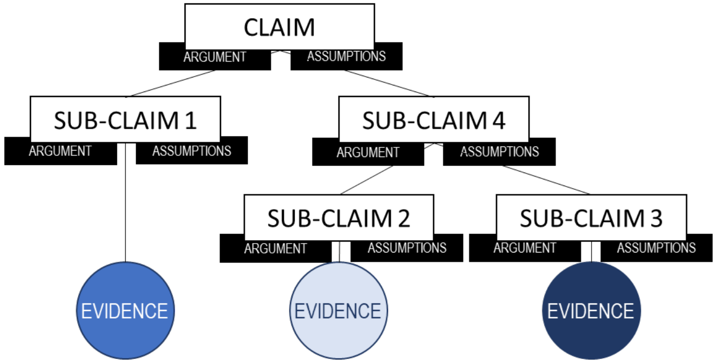
Identify Threats, Risks, Vulnerabilities in the context of the system
Identify Component Threats, Risks, Vulnerabilities
Evaluation of Risk
Assess & Apply Mitigations
Evaluation of Risk
Assess & Apply Mitigations

USE – PROGRAMMATIC GUIDANCE

- What is the impact to my DoD system of using a part with the identified risks?
- Is the assurance case for the CIC or FPGA commensurate with my system needs? If not, how should they be tailored?
- Does the COTS component meet my assurance needs? If not, can I select another part?
- Are additional, system-level mitigations warranted?
- ME Lifecycle Elements: Programming through Operations and Maintenance

- Threat models are separate but interlocking.
  - Both adhere to common risk process (identify threats, apply mitigations, evaluate risk).
  - Standardization of MAKE model would enable link to digital engineering representation of DoD system (USE).
  - Support defense in depth via tailoring of requirements, scaling of evidence in MAKE threat model (CIC, FPGA).

A key Standard element: Assurance Cases



IF ● **THEN** sub-claim 1; **IF** ○ **THEN** sub-claim 2; **IF** ● **THEN** sub-claim 3;
IF sub-claim 2 and sub-claim 3 **THEN** sub-claim 4; **IF** sub-claim 1 and sub-claim 4 **THEN** CLAIM

An assurance case includes a top-level claim for a property of a system or product (or set of claims), systematic argumentation regarding this claim, and the evidence and explicit assumptions that underlie this argumentation.

- **The benefits of utilizing assurance cases include:**
  - **Fidelity of model is improved by explicitly including justification, evidence, and assumptions.**
  - **Interconnectivity of model supports improved understanding, use by DoD programs and industry.**
  - **Encourage development of automation, tools based on assurance cases to improve scalability, automation.**
- **OUSD (R&E) has indicated that they are already exploring use of assurance cases.**

DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited

Section IV:

RECOMMENDATIONS

Executive Summary: Recommendations

1. Ensure DoD access to the commercial ME supply chain, domestically and with allied nations.
2. Adopt best practices and standards to mitigate risks.
3. Create Microelectronics Assurance for National and Economic Security (MANES) for synergies between TF and MQA to mitigate mutual weaknesses and strengthen overall ME Assurance posture.
4. Embrace overlays over commercial processes and create a variety of options to meet DoD program requirements.
5. Accelerate investment in MQA and overlay development.
6. Embrace Design for Assurance for defense-in-depth.
7. Accelerate the maturity of MANES.
8. Create an integrated standards framework for acquiring ME parts through overlays and their deployment in DoD systems.
9. Build and resource the DoD ME Assurance governance and cooperative structures: The MANES Executive Agent and the MANES Standards Board.
10. Create ME Assurance Standards Board to plan for the creation, deployment & evolution of standards and guidance.
11. Align CHIPS with MANES Needs.
12. Ensure adequate funding and resourcing for MQA and all current and future entities

Rec 1: Ensure DoD Access to the commercial ME supply chain

- Leverage commercial ICs and FPGAs to the maximum extent possible.
- Continue to leverage artifacts and content from existing best in-class commercial processes for evaluating assurance and maturing MQA.
- Implement commercial best practices while MQA guidance is maturing, including publication of interim guidance.
- Engage commercial fabs to gain access to artifacts and content currently not available to assurance evaluators.
- Develop defense-in-depth approaches.
- Incentivize programs to take advantage of early commercial supply chain for assured microelectronics.
- Support workforce development.

DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited

Rec 2: Adopt best practices to mitigate risks

- DoD should:
  - Develop and deploy assurance methods to evaluate and manage risk associated with using commercial microelectronics.
    - To ensure a sufficiently robust supplier pool, these methods must work smoothly within the commercial microelectronics ecosystem.
  - Focus investment on mitigations applied to lifecycle stages with the highest risk.
    - Investments should prioritize design, assembly, packaging, testing and configuration and programming.
    - Heightening assurance and/or security for mask and wafer fabrication should not be the priority for investment.
    - A cost-aware assessment (e.g., ALARP) should be used to understand the optimum balance of mitigations for a range of assurance needs.
  - Manage risk across the entire microelectronics lifecycle for each DoD program.

Rec 3: MANES: Alignment between TF and MQA

- Dispel confusion by adopting a new term MANES. Create unity of approach.
  - MANES includes confidentiality, integrity, and availability aspects.
  - MANES allows the DoD to tailor the assurance mitigations to programmatic needs when utilizing commercial parts or commercial flows.
- Adopt MANES, which encompasses a set of overlay flows to meet the risk mitigation needs of a program:
  - TF for classified parts.
  - ITAR/EAR for controlled parts.
  - MQA for high integrity.
- Implement the above methodologies on top of commercial best practices. Methodologies succeed or fail based on underlying systems and the underlying systems must fill gaps in either methodology.
- Continue using TF access for confidentiality while maturing MQA for integrity. Make both available to DoD programs.

Rec 4: Embrace overlays

- Overlays over commercial flows offer the DoD the flexibility to tailor commercial parts to program requirements.
- Incentivise industry to offer three overlay options:
  - MQA, ITAR, Classified.
- Invest in the creation and enablement of overlays using guides and standards.
- Make the options easily accessible to programs.
- Ensure that the DoD has access to multiple providers of the three types of overlays.
- Ensure compliance and evolutionary ME assurance improvements by augmenting commercial processes with independent expert assessments.

Rec 5: Accelerate MQA development

- DoD should:
  - Accelerate the investment in and the tempo of the MQA pilots.
  - Work with semiconductor IP community to establish cost effective method to support the evaluation of assurance.
  - Coordinate MQA development with Dept of Commerce/CHIPS efforts to establish commercial supply chain security, such that they can be leveraged for DoD use.
  - Invest to lower and/or remove legal and technical barriers to IP data sharing and protection of shared data.
  - This review focused on digital custom integrated circuits, in the scope of FinFET or newer devices (<12 nm).
  - DoD should extend this analysis to other important microelectronics technologies (e.g., analog, mixed signal, RF, legacy CMOS, COTS).

Rec 6: Design for Assurance

- Embrace defense in depth. DoD should continue to fund development of “Design for Assurance” (DfA) techniques to reduce the need for manufacturing mitigations for confidentiality, integrity, and availability.
- MANES should incorporate an up to date understanding of commercially available DfA techniques to create resilient designs that reduce the downstream assurance requirement. This is an evolving topic, but examples of best practices include:
  - Protecting critical IP by separating from the hardware and inserting as software after manufacture where possible.
  - Establishing and utilizing methods to extend post-silicon test including testing of “dark” circuitry for critical devices (e.g., picosecond imaging circuit analysis (PICA), thermal measurement) and negative testing.
  - Incorporating “canary” structures can serve as out of band validation for some critical manufacturing elements.
  - Incorporating sensors that can enable monitoring of parametric data.
  - Incorporating an immutable chip ID that is enrolled in a secure database as early as practicable in the supply chain can mitigate against the use of counterfeits.
  - Incorporating run-time validation efforts (e.g., Logic built-in self-test, LBIST) can improve confidence in integrity of device function.
  - Incorporating security features supporting resilience in fielded microelectronics: Security subsystems that isolate and protect critical functions, secure boot, update and debug, use of cryptographic methods, and run-time integrity protections.
  - DfA techniques should be synergistic with anti-tamper ones to enhance system resilience.

Rec 7: Accelerate the maturity of MANES

- Continue to support existing and additional assurance development pilot programs – USD(R&E).
  - Each pilot should result in products that support maturation and dissemination of data standards, data analytics, guidance, and best practices.
- Include demonstrations for both parts manufacture and deployment – MQA pilots.
- Develop tools, techniques, and technology to support scalability and automation, including cost effective automated data collection and analytics.
  - If the DoD, Intelligence Community, DoE are going to request data for evidence, the data request (what and format) need to be standardized – each USG program should not be asking for different data (or in different formats).
- Require a cost-aware assessment (e.g., ALARP) to understand the optimum balance of data-and human-centric mitigations for a range of assurance needs – DoD.
- Guidance should be published incrementally – as it becomes available – and updated regularly.
  - Guidance may establish requirements for mature mitigations (e.g., commercial best practices) while DoD data analytic capability is matured.
  - Consider phased adoption of MANES assurance cases.

DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited

Rec 8: Develop a two-part ME Assurance Standard

- Create a two-part Microelectronic Assurance Standard.
  - Part 1: Microelectronics lifecycle standards for making parts
    - Establishes assurance cases for the three different types of overlays: commercial, export controlled and classified.
    - Establishes assurance cases for each overlay.
    - Suppliers can choose to satisfy any or all assurance cases.
  - Part 2: Programmatic guidance for using parts.
    - Guides DoD programs in managing microelectronics assurance risk associated with their systems.
      - Adopt and tailor assurance cases commensurate to program security requirements for DoD custom designs (e.g., CIC, FPGA application design).
      - Evaluate risk of available COTS parts based on relevant assurance cases; develop and deploy additional mitigations as necessary.
- Include COTS devices in ME Assurance guidance.

Rec 9: Create a MANES Executive Agent

- Establish a MANES Executive Agent (EA) along the same lines and as a counterpart to the Anti Tamper (AT) Agent and locate it in one of the Services:
  - The MANES EA focuses on the microelectronics part during its creation and connects programs with assured parts:
    - Define the mission – suggested mission: Assurance Threat Analysis, Policy & Procedures, Assurance Plan Evaluation, Assurance Assessment, Assurance Education & Outreach, Acquisition Support, Data Repository.
    - Work with other groups to develop and implement standards – government and industry stakeholder council.
    - Facilitate access to SOTA ME by aggregating demand, use of multiple project wafers, etc. – similar to TAPO/DMEA functions.
    - Facilitate transition and implementation of MANES methodology to acquisition and sustainment systems.
  - The AT Agent focuses on the part during its operation as part of a DoD system and manages risk during the lifetime of deployment of the part into a system.

Rec 10: ME Assurance Standards Board

- Plan for the creation, deployment & evolution of standards and guidance by creating ME Assurance Standards Board hosted/led by NSA in collaboration with OUSD(R&E), OUSD(A&S) and the Services.
- Works in tandem with the MANES Executive Agent.
- Suggested Board Charter:
  - Draft the standard confidentiality and integrity standards.
  - Develop community consensus.
  - Enable interim application of the standards.
  - Evaluate deployment and support evolution.
- Members must include government, the DIB, the semiconductor industry and academia.
- Responsible body for managing the evolution:
  - Example:
    UK MOD Safety and Environmental Standards Review Committee (SESRC).
  - Example of evolution of a standard:
    UK MOD management of DefStan 00-056 (Safety Management Requirements for Defence Systems).

Rec 11: Align CHIPS with MANES Needs

- The CHIPS Act was enacted and funded to onshore ME manufacturing *to protect national and economic security.*
- DoD needs assured *access* to performant ME manufacturing capabilities that (to varying degrees) protect the *integrity* and *confidentiality* of the product.
- The CHIPS Act aims to increase the *domestic supply* of such parts.
- CHIPS Act should be leveraged to address *National Security needs.*
- Ensure the coordination with DoD includes support to MANES efforts:
  - Include access to the data.
  - Incentivize commercial suppliers to offer MQA, ITAR/EAR and classified overlays through CHIPS infrastructure funding.
  - Apply CHIPS R&D funding to support objectives of MANES.
  - Continue to support workforce development for MANES.
- *Standards*, paired with *policy modernization*, are the key to enabling the *DoD warfighter* to take advantage of the domestic supply created by CHIPS.

Rec 12: Ensure adequate funding and resourcing

- Ensure adequate funding and resourcing for the following current and future entities:
  - MQA
  - MANES
  - MANES EA
  - ME Assurance Standards Board
  - JFAC Hardware Assurance Labs to support MANES
  - DMEA
  - Programs [to enact MANES]

DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited

Returning to The Key Questions

- What are the national security implications of increasing our use of commercial microelectronics fabrication flows relative to the use of Trusted Foundry flows?
  - Access to commercial ME is essential for obtaining performant, trustworthy and affordable parts to create mission capable DoD systems. Not having access threatens our national security.
- What are the risks entailed?
  - The risks include compromise to confidentiality, integrity and availability of function of ME devices. These risks are lower during mask and wafer fabrication and higher during design, testing and configuration. ME is not free of risk but is not the greatest risk by far.
- How can we mitigate these risks in a practical way?
  - Risks can be mitigated by creating a rational ME Assurance risk management regime, combining TF with MQA overlays over commercial practices, designing for assurance/defense in depth, and creating and implementing standards.
- Will the risk reduction be enough?
  - There is no perfection but the risk can be managed to be as low as reasonably practicable.
- How are we going to implement in practice a viable risk reduction regime?
  - By creating the ME Assurance EA, the ME Assurance Standards Board, by resourcing the ME Assurance governance appropriately and by aligning execution of the CHIPS program with DoD needs.

ACKNOWLEDGEMENTS, DEFINITIONS & ACRONYMS

Acknowledgements: MQA Review Panel Members

Name	Position*	Home Organization*
Dr. Victoria Coleman	Panel Chair, Air Force Chief Scientist	Department of the Air Force
Prof. Krste Asanović	Prof Electrical Eng & Comp Sciences	University of California, Berkeley
Mr. Kerry Bernstein	Principal Scientist	Modern Tech Solutions, Inc.
Dr. Gerry Borsuk	Associate Director of Research for Systems	Naval Research Laboratory
Dr. Meredith Dyck	Chief Strategist, Microelectronics	National Security Agency
Mr. Frank Ferrante	Vice President Automotive Sales & Marketing	Wolfspeed
Dr. Craig Fields	Retired, former Defense Science Board Chair	Independent
Mr. David Flowers	Microelectronics Sector Lead	OUSD – Acquisition & Sustainment
Mr. Jim Gosler	Senior Fellow, Applied Physics Lab	Johns Hopkins University
Ms. Deirdre Hanford	Chief Security Officer	Synopsys
Mr. Adam Hauch	Supply Chain Awareness & Security Technical Lead	NSWC - Crane Division
Mr. Jeffrey Krieg	Chief, Hardware Reverse Engineering	National Security Agency
Dr. Jay Lewis	Office of the CTO, Strategic Mission Technologies	Microsoft
Mr. James P, Libous	Retired, Lockheed Martin Fellow, CTO Office	Independent
Dr. John Manferdelli	Security, Office of the CTO	VMWare
Dr. Michael Mayberry	Retired, former Intel CTO	Independent
Dr. Christine Michienzi	Senior Technology Advisor for the USD A&S	OUSD – Acquisition & Sustainment
Mr. Andreas Olofsson	CEO at Zero ASIC	Zero ASIC
Mr. Steve Orrin	Federal CTO & Senior Principal Engineer	Intel Corporation
Ms. Nicole Petta	Senior Director, Strategic Operations	Qualcomm
Ms. Kaila Raby	Senior Manager of Advanced CMOS Solutions	Sandia National Laboratories
Mr. Keith Rebello	Senior Technical Fellow	Boeing
Mr. Glen (David) Via	Anti-Tamper Executive Agent Technical Director	USAF SAF/AQ
Mr. Walter Weiss	CTO	OUSD – Intelligence & Security
Dr. Bob Wisnieff	CTO Quantum Computing	IBM, Defense Science Board
Prof. H.-S. Philip Wong	Prof. of Electrical Engineering	Stanford University
Dr. John Zolper, Sr.	Defense Technology Strategy	Raytheon Technologies

* Note that panel members from industry and academia were appointed as Special Government Employees for the purposes of the MQA Review Panel

Acknowledgements: Acq Reps, Advisers, Support

Acquisition System Representatives

Name	Position	Organization
Mr. Ted Bujewski	Engineering Lead	USSF SAF/SQ
Dr. Donna Joyce	Army Protective Technologies ST	US Army
Dr. Michael Steinbock	Microelectronics Lead	USSF SAF/SQ
-	-	US Navy acquisition declined to take part

Advisers

Name	Position	Organization
Ms. Stephanie Lin	Systems Engineer	OUSD – Research & Engineering
Ms. Christine Rink	Microelectronics Lead Policy Analyst	OUSD – Research & Engineering
Dr. Jason Vosatka	Senior Security & Electronics Engineer	48th Cyberspace Test Squadron, USAF

Support Team

Name	Position	Organization
Maj Andrew Beauchamp, PhD	Special Assistant to the USAF Chief Scientist	USAF AF/ST
Mr. Chris Bozada	Division Technical Advisor	AFRL/RYD
Mr. Ryan Clay	UK Special Assistant to the USAF Chief Scientist	USAF AF/ST
Dr. Brett Wenner	Senior Research Scientist and Special Project Lead	AFRL/RYD

Acknowledgements: Briefings to the panel (1/2)

Name	Briefing Topic	Role, Organization
Dr. Craig Fields	MQA Study Scene Setting	Independent
Dr. Dev Shenoy	Overview of T&AM projects (SHIP/RAMP/RAMP-C)	Principal Microelectronics Dir, OUSD(R&E)
Dr. Matthew Kay	Overview of T&AM efforts in MQA	Trusted Microelectronics Chief Engineer, NSWC Crane
Dr. Gerry Borsuk	Out-brief of the Defense Microelectronics Advisory Group's (DMAG) study of MQA	Associate Director of Research for Systems, NRL
Ms. Christine Rink & Col Matt Spencer	MGUE Program Overview/Lessons Learned	MGUE Program
Dr. John Manferdelli	Out-brief of DSB Microelectronics Report	Defense Science Board
Mr. James Inge & Mr. Dewi Jones	UK MOD Def Stan 00-056: Safety Management Req's for Defence Systems – Principles, Development & Application	UK MOD Defence Equipment & Support
Dr. Nick Martin	DMEA Trusted Foundry	DMEA Director
Prof. H.-S. Philip Wong	TSMC: Management of Assurance in Fabrication	Prof. of Electrical Engineering, Stanford
Mr. Joe Tostenrude	RAMP Phase 2 MQA Update	Director, Customer Engagements (RAMP TPM Lead), Microsoft
Ms. Chris Irvine	Intro to Qualcomm Quantifiable Assurance Efforts	Principal Engineer, Qualcomm Tech Inc.
Mr. Ryan Clay	Royal Air Force real world example of As Low As Reasonably Practicable (ALARP) Principal	UK Exchange Special Assistant to the USAF Chief Scientist, USAF AF/ST
Ms. Krystal Donald	Field Programmable Gate Array (FPGA) Levels of Assurance (LoAs)	JFAC FPGA Assurance Team, NSA
Prof. Krste Asanović	RISC-V and MQA	Chairman, RISC-V International; Co-Founder and Chief Architect, SiFive Inc.
Mr. Ife Hsu	Intel - MQA Standard Briefing	Technology/Development Manager, Corporate Quality Network, Intel
Dr. Anna Melker	Classified NSA Threat	Laboratory for Physical Sciences
Mr. Walter Weiss	Classified CHIPS Overwatch	CTO, OUSD(I&S)
Dr. Caitlin Friedman	Classified SOTA Assurance Gaps/Challenges	Sandia National Laboratories

DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited

Acknowledgements: Briefings to the panel (2/2)

Name	Briefing Topic	Role, Organization
Dr. Anna Melker	Classified NSA Threat	Laboratory for Physical Sciences
Mr. Walter Weiss	Classified CHIPS Overwatch	CTO, OUSD(I&S)
Dr. Caitlin Friedman	Classified SOTA Assurance Gaps/Challenges	Sandia National Laboratories
Mr. Ezra Hall	RAMP/SFA/MQA and DoD Implementation	Senior Director WorldWide Aerospace & Defense, GlobalFoundries
Mr. Neil Schumacher	Trusted Foundry & Quantifiable Assurance	Client Executive, IBM Consulting Service
Dr. Linton Salmon	MQA	Technical Advisor to the Principal Microelectronics Director, OUSD(R&E)
Dr. Shamik Das	MQA Independent Assessment	Chief Engineer, OSD Programs, The MITRE Corporation
Ms. Xochitl Monteon	Threats to ME Design and Fab Process	Chief Privacy Officer/VP Cybersecurity Risk & Governance, Intel Corporation
Dr. Chris Taylor	RAMP MQA Data Assessment	Senior Research Scientist, Battelle Memorial Institute
Mr. Jody Defazio	Assurance & IP Product Development	Vice President, IP Quality/Functional Safety/Cybersecurity, Synopsys
Dr. Sergiu Ghetie	Demonstration of Cybersecurity & Supply Chain Attacks	Founder & CEO, Cloud Tank, Inc.
Mr. Glen (David) Via	Microelectronics Evidence Based Assurance (MEBA) Executive Agent Strawman Concept	Anti-Tamper Executive Agent Technical Director, USAF SAF/AQ
Mr. Jeff Krieg	DoD FPGA Assurance Strategy Overview	Chief, Hardware Reverse Engineering, NSA

Definitions (1/2)

Definitions for the purpose of this presentation

Term	Definition
Access	The ability of the DoD to obtain parts in a timely, cost-effective way to satisfy programmatic needs
ALARP	As Low As Reasonably Practicable – a level of risk below which the sacrifice involved in the measures necessary for further averting the risk (whether in money, time or trouble) is grossly disproportionate to the quantum of risk averted
Assurance (microelectronics assurance)	A level of confidence that a part will perform its function (and nothing else) when called upon to do so and do so without exposing protected data or IP – collectively refers to *Confidentiality*, *Integrity* and *Availability* (CIA) properties.
Assurance Case	A reasoned, auditable artifact created that supports the contention that its top-level claim (or set of claims), is satisfied, including systematic argumentation and underlying evidence and explicit assumptions that support the claim(s) (via NIST)
Availability	The device/system is available to execute its mission when called upon to do so; there has been no alteration during the lifecycle that would impact the availability of the device to perform its function.

DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited

Definitions (2/2)

Definitions for the purpose of this presentation

Term	Definition
Confidentiality	Confidence that all access to devices or design artifacts is authorized
Integrity	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 (derived from DAU definition for hardware assurance)
MANES	[New term introduced in this review] Microelectronics Assurance for National and Economic Security – the practice of ensuring a level of assurance commensurate with program requirements is achieved via establishing and executing appropriate microelectronics assurance cases
MQA	Microelectronics Quantifiable Assurance – a method of evaluating and quantifying microelectronics assurance risks to support program-specific, risk-based decision making
Trusted	Accredited by DMEA
Flow	The collection of steps and processes used in designing and manufacturing an IC

DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited

Acronyms (1/5)

Acronyms for the purpose of this presentation

3PIP	Third-party intellectual property
ALARP	As low as reasonably practicable
ASIC	Application-specific integrated circuit
CDD	Capability Development Document
CDR	Critical Design Review
CHIPS	Creating Helpful Incentives to Produce Semiconductors Act
CIC	Custom integrated circuit
CMOS	Complementary metal oxide semiconductor
COTS	Commercial off-the-shelf
CUI	Controlled Unclassified Information
DfA	Design for Assurance

Acronyms (2/5)

Acronyms for the purpose of this presentation

DfA	Design for Assurance
DIB	Defense Industrial Base
DMEA	Defense Microelectronics Activity
DoC	Department of Commerce
DoD	Department of Defense
DoE	Department of Energy
DTSA	Defense Technology Security Administration
EA	Executive Agent
EAR	Export Administration Regulations
EDA	Electronic design automation
FinFET	Fin field-effect transistor

DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited

Acronyms (3/5)

Acronyms for the purpose of this presentation

FPGA	Field programmable gate array
IC	Integrated Circuit
IP	Intellectual property
IT	Information technology
ITAR	International Traffic in Arms Regulations
JROC	Joint Requirements Oversight Council
LBIST	Logic built-in self-test
MANES	Microelectronics Assurance for National and Economic Security
ME	Microelectronics
MGUE	M-Code GPS User Equipment
MQA	Microelectronics Quantifiable Assurance

DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited

Acronyms (4/5)

Acronyms for the purpose of this presentation

MSI	Miniature Serial Interface
NDA	Non-disclosure agreement
PDR	Preliminary Design Review
PICA	Picosecond imaging circuit analysis
RAMP	Rapid Assured Microelectronics Prototypes
RF	Radio frequency
RFP	Request for proposals
RTL	Register-transfer level
SCIF	Sensitive compartmented information facility
SCRM	Supply chain risk management
SoC	System on Chip

DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited

Acronyms (5/5)

Acronyms for the purpose of this presentation

SOTA	State of the art
SOTP	State of the practice
SWaP	Size, weight and power
TAPO	Trusted Access Program Office
TF	Trusted Foundry
USG	United States Government
V&V	Verification and validation

DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited

UNITED STATES AIR FORCE

CHIEF SCIENTIST

DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited.