Microelectronics Quantifiable Assurance (MQA) Independent Assessment

Shamik Das, Ph.D.
Assessment Team Lead
Chief Engineer, OSD Programs
The MITRE Corporation

1 March 2023

Copyright © 2023 and all rights reserved by the authoring corporations unless otherwise indicated.

Executive Summary

- An independent team was convened to assess the technical viability of the Microelectronics Quantifiable Assurance (MQA) framework under development by OUSD(R&E)
- Conclusions of the assessment team are as follows:
  - MQA represents a good-faith standards and practices initial/partial technical solution to provide ME sourcing flexibility to DoD targeting Congressional and DoD intent
  - MQA is <u>not ready for deployment</u> in present form, but could be made to work
  - Significant gaps exist rendering MQA <u>an incomplete solution</u> for addressing threats
  - Focused near-term attention and investment are needed to ensure:
    - Sufficient alignment with Service/Component acquisition and sustainment pathways
    - Cogent communication and training on MQA
    - Efficient multilateral collaboration between DoD and industry participants
    - Timeliness of MQA completion so that it can be used when relevant commercial capabilities come online

Outline

- Objectives and Key Questions for the Assessment
- Independent Definitions Established by the Assessment Team
- Summary of Key Findings and Recommendations
- Conclusions and Next Steps
- Appendix: Detailed Exposition of Findings

Objective of This Assessment

OUSD(R&E) requests an independent, unbiased evaluation to be conducted of the Microelectronics Quantifiable Assurance (MQA) methodology under development in OUSD(R&E)'s Trusted and Assured Microelectronics (T&AM) program.

The Independent Assessment Team will:

- Provide an independent, objective view of the progress of MQA development toward meeting the objectives laid out in the NDAA and elsewhere
- Evaluate the scientific and technological claims asserted by MQA documents regarding security and capability of the components to be acquired via MQA
- Obtain data from pilot programs supporting or refuting these claims
- Obtain viewpoints from stakeholders both within and outside of the defense community

Key Questions

- What is MQA? i.e., provide an unbiased definition/specification of MQA, provide a statement of what was intended by Congress via legislation, and assess what capabilities and components MQA is intended to incorporate or enable.
- What are the specific needs that MQA is addressing and what will not be addressed? If a need is not addressed by MQA, is there an existing mechanism to address that need or is there a gap?
- Can the proposed MQA framework and methodology provide DoD with the equivalent of assured access to trusted microelectronics? Will MQA enable the DoD to obtain levels of security, assurance, and/or program protection exceeding that provided via the Trusted Foundry model?
- Will MQA provide programs with microelectronics whose performance (e.g., speed, power, other application-specific figures of merit) exceeds that available via existing Trusted Foundry capability, and if so, to what extent (i.e., can the increase in available performance be quantified)? What will be the resulting system performance impact to weapon systems?
- Does MQA put forward a set of standards that meet the requirements and intent of the 2020 NDAA Section 224?
- Are the MQA tools and standards compatible with industry supplier practices, such that multiple suppliers at the state of the art are expected to engage with DoD using the MQA framework so as to be available for sourcing of components? What measures will be put in place to ensure or monitor industry compliance with agreed-upon standards?
- Does the proposed MQA approach take advantage of or work compatibly with similar practices adopted already by commercial industry to ensure the security and integrity of their products?
    - What practices does industry implement to achieve security (confidentiality, integrity, availability) in their products? Do commercial manufacturers have any quantitative measures they customarily apply?
    - What commercial standards exist currently in this space that are industry-originated and/or widely adopted or respected by commercial suppliers?
- What is the role/charter of JFAC as relates to executing the MQA methodology? If that role/charter is not clearly defined, what is required?

Methodology: Assessment by Lines of Effort

1. An evaluation of the overall MQA approach, as documented in draft DoDI 5200.XX, associated guidebooks/manuals, and other program documentation, to assess viability for procuring microelectronics for DoD use cases

2. An evaluation of the MQA's Attack-tree Countermeasure Analysis (ACMA) methodology for its viability in assessing risk and identifying mitigations

3. ~~A comparative utility assessment of the supply-chain tools, e.g., AMARO, to be used, applied, or furnished by DoD to vendors for conducting risk assessment of the commercial manufacturing supply chain to be involved in prospective microelectronic component manufacturing~~ [OBE per discussion with the Gov't team at task kickoff]

4. An evaluation of data and evidence being generated by RAMP, RAMP-C, ~~and SHIP~~ pilot programs to demonstrate the viability of the MQA method
   - Evidence will include but is not limited to technical performance of the microelectronics being fabricated via these pilots, in comparison with leading-edge commercial off-the-shelf capabilities for general-purpose and special-purpose microelectronics
   - This evaluation will include assessment of impacts/mitigations should the data be unavailable or insufficient to execute the MQA methodology as intended

5. An assessment of technical capabilities likely to be afforded by MQA and identification of any gap areas that will need to be fulfilled via RAMP-C, Trusted Foundry, or other approaches

6.-8. An evaluation of DoD- and IC-wide posture regarding acceptance/adoption of proposed MQA policy, compatibility with existing and anticipated missions, and degree of coordination/collaboration to implement MQA

Technical Lines of Effort and Teaming Arrangement

Line of Effort	Lead	Team Members
1. Policy and standards	JHU APL	Draper, GTRI, Sandia
2. ACMA methodology	Draper, GTRI, Sandia	GTRI, JHU APL, MITRE, Sandia
~~3. Tools assessment~~	~~Draper, MITRE~~	~~Draper, GTRI, MITRE, Sandia~~
4. Pilot programs	MIT LL, Sandia (RAMP)	GTRI, JHU APL, MITRE, Sandia
5. Technical impact of MQA (e.g., PPAC)	MITRE	Draper, GTRI
6. USG stakeholders (A&S, PORs, SAEs, etc. DoD as well as IC and other USG)	Draper, Sandia	Draper, GTRI, IDA, MITRE
7. Other stakeholders (private industry), including 3PIP topic	Draper, IDA	Draper, JHU APL, MITRE
8. Mission thread analysis	GTRI	Draper, MITRE
Overall findings/reporting/etc.	MITRE	Draper, GTRI, IDA, JHU APL, MIT LL, Sandia

What is Microelectronics Quantifiable Assurance (MQA)?

What is MQA? —Definition by the Independent Team

MQA is a threat-specific, risk-accumulative approach to conducting a technical assessment of the potential for adversarial induced failure or compromise of a microelectronic component intended for use in a DoD weapon system or platform. MQA leverages Attack-Tree Countermeasure Analysis (ACMA) in component development pathways targeting (1) custom integrated circuits (CIC), (2) field-programmable gate arrays (FPGAs), and (3) commercial-off-the-shelf (COTS) components.

Further, MQA presently is:

- Tailored to the specifics of the design-to-product value chain (e.g., for CIC, where the component is designed; where the masks are produced; where the chip itself is fabricated; who does the packaging, assembly, and test)
- Based on anticipatory, possible, or hypothetical threats/risks (informed by reason), instead of being weighted by prior incidence or experience of actual threats
- Tabulated based on an unweighted tally of risk mitigators selected from a pre-defined corpus
- Intended for subjective evaluation of the risk by a third party (e.g., JFAC), whose practitioners are SMEs but not subject to independent certification or qualification

Standards Enabling MQA – 2020 NDAA Sec. 224

(b) TRUSTED SUPPLY CHAIN AND OPERATIONAL SECURITY STANDARDS.—

(1) STANDARDS REQUIRED.—(A) Not later than January 1, 2021, the Secretary shall establish trusted supply chain and operational security standards for the purchase of microelectronics products and services by the Department.

(B) For purposes of this section, a trusted supply chain and operational security standard—

(i) is a standard that systematizes best practices relevant to—

(I) manufacturing location;

(II) company ownership;

(III) workforce composition;

(IV) access during manufacturing, suppliers' design, sourcing, manufacturing, packaging, and distribution processes;

(V) reliability of the supply chain; and

(VI) other matters germane to supply chain and operational security; and

(ii) is not a military standard (also known as "MIL-STD") or a military specification (also known as "MIL-SPEC") for microelectronics that—

(I) specifies individual features for Department of Defense microelectronics; or

(II) otherwise inhibits the acquisition by the Department of securely manufactured, commercially-available products.

Standards Enabling MQA

- MQA standards meet the definition/requirement of a technical standard, e.g., for an electronic interface or software language
  - Prescriptive with respect to what threats ought to be considered
  - Prescriptive regarding best practices that are available to address threats

Standards are commercially compatible and systematize DoD's view of best practices, thereby satisfying these aspects of 2020 NDAA Sec. 224

- The standards need further specification: compliance does not lead to a deterministic program decision or outcome
  - Different programs can apply MQA identically yet achieve differing go/no-go decisions
  - Contrast with: use of Trusted Foundry satisfying DoDI 5200.44
  - Contrast with: ISO 9001, DO 254
  - No entity (including the JFAC) has been given independent audit authority to certify that MQA has been applied correctly, consistently, or in accordance with policy or technical best practices

Standards are not suitably prescriptive for independent commercial use or certification, so are not likely to lead to broad adoption for non-DoD customers

Key Findings and Recommendations

Key Findings

1. MQA is not quantifiable as currently articulated
2. MQA is not specified equally for all applicable acquisition pathways
3. Pilot program activities highlight scalability issues with MQA
4. For major capability acquisitions, MQA might be applied with minimal impact to cost and schedule – but also limited upside to performance
5. Stakeholders exhibited limited knowledge or exposure to MQA and expect limited utility from MQA under present conditions

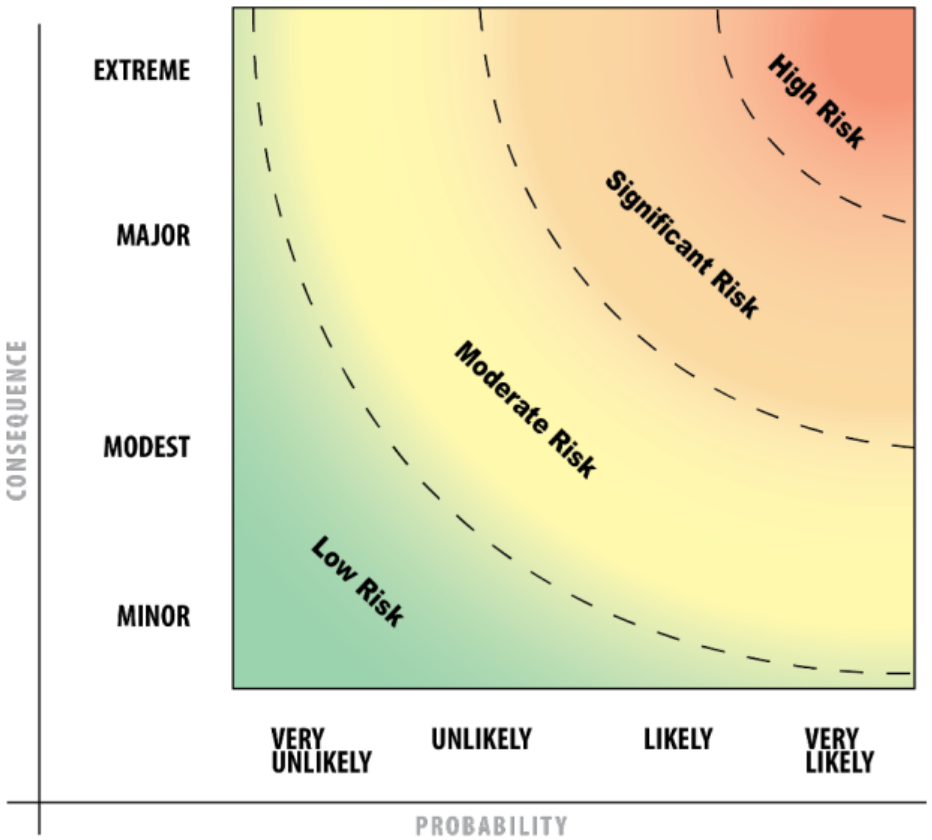
Significant additional R&D work and outreach are required to make MQA viable for use by Programs and provide added value to commercial industry

1. MQA is not Quantifiable as Currently Articulated

- Risk is commonly assessed as a combination of Probability (Likelihood) and Consequence
- MQA comprehends Consequence in terms of required Level of Assurance
- MQA does not quantify Likelihood – instead, treats all threats as needing mitigation
  - Most likely because this is hard
  - Also, most threats tabulated for CIC are low-likelihood compared with counterfeiting or other component-level supply-chain issues
- Program Manager is left to evaluate which microelectronic threats are severe and which mitigations are sufficient

LoA 2

LoA 1



??? Unquantified ???

Figure source: *Joint Risk Analysis Methodology*, CJCSM 3105.01A, 12 Oct. 2021

MQA's Implementation of ACMA Is Also Not Quantitative

MQA high-level implementation:	Concerns:
• Identify Threats →	• Threat likelihood is not assessed
• Apply Mitigations →	• Some mitigations are not prescriptive or quantitative
• Assess Residual Risk →	• Risk assessment is subjective and left to Program

Qualitative decisional aspects of MQA fall short of what is expected for compliance and certification in commercial standards

Summary of Findings with Respect to ACMA

- Significant gaps exist in the current MQA implementation of ACMA for both CIC and FPGA threat scenarios
- ACMA mitigations lack actionable specificity
- The ACMA process and implementation provide insufficient guidance for residual risk quantification
- Differentiation of defined threats between Levels of Assurance (LoAs) are undefined

Custom Integrated Circuit (CIC) Threat Tier vs. Stoplight Rating	Red – Threat Not Mitigated	Yellow – Partial Mitigation	Green – Threat Mitigated
Tier 1 – Direct Component Compromise	**2**	**10**	4
Tier 2 – Significant Programmatic Effect	**3**	**2**	0
Tier 3 – Design Data Leakage	0	5	4
Tier 4 – No Component Compromise or Design Data Leakage	2	0	2

Field Programmable Gate Array (FPGA) Threat Tier vs. Stoplight Rating	Red – Threat Not Mitigated	Yellow – Partial Mitigation	Green – Threat Mitigated
Tier 1 – Direct Component Compromise	**1**	**6**	5
Tier 2 – Significant Programmatic Effect	**1**	**3**	0
Tier 3 – Design Data Leakage	0	0	0
Tier 4 – No Component Compromise or Design Data Leakage	0	0	0

Recommendations Regarding Technical Threat Mitigation

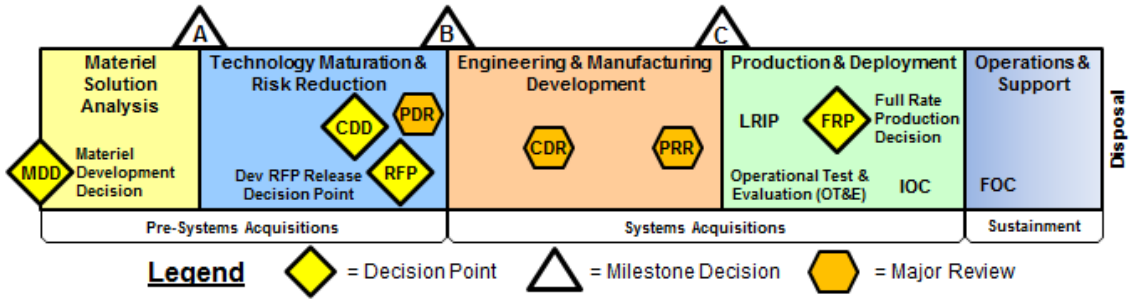
- Develop Digital Engineering framework (possibly commercial dual-use) and Post Silicon Mitigation ecosystem (via DoD or DIB) that can be used for the entire Department
- Address and articulate threats/mitigations that account for field updates of FPGAs
- Articulate procedures for incorporating vendor-developed technical mitigations to USG-defined threats (e.g., novel obfuscation or anti-counterfeiting techniques) and quantifying the residual risk
- For guidebook documentation:
  - Expand upon the mitigation descriptions
  - Ensure that they are clearly defined and provide sufficient guidance on actions to take
  - Provide exemplars of data products associated with each mitigation
- Articulate a strategy for quantifying and managing residual risk if:
  - One or more mitigations are not able to be fully implemented by programs
  - Mitigations identify an emergent risk during fabrication or testing – see next slide
- Document the process for the incorporation of threats and mitigations into the current and future ACMA versions
- Ensure the CIC and FPGA implementations are consistent across the documentation

Special Note Regarding Emergent Risks

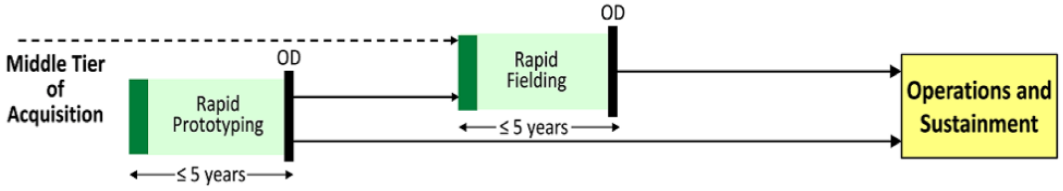
- By design, some MQA mitigations involve assessment of data produced during the component fabrication process
- This can result in risks being identified several months or years into a program's acquisition cycle
- The PM/MDA have the authority to evaluate the severity of this risk and will be expected to make go/no-go decisions trading off this risk against cost and schedule pressure of mitigation
- In past instances of safety-critical systems this has led to severe consequences, up to and including loss of life, when SME technical objections were overruled in favor of meeting program milestones
  - For mission-critical systems, the PEOs interviewed for this assessment all preferred a risk-averse posture (i.e., using mature, proven microelectronics technology that favors mission readiness vs. using a new technology that provides higher capability but might risk successful execution)

2. MQA is not Specified Equally for All Applicable Acquisition Pathways

- Major capability acquisitions already conduct SME-based risk assessments
- Timeline from concept development to production to fielding is much longer than semiconductor industry's cadence (5-10 years vs. 2-3 years)
  - Therefore, MQA <u>would not</u> bring state-of-the-art microelectronics to major weapons systems
  - However, MQA <u>could</u> bring to bear assurance technologies that are not available via traditional Trusted pipelines
- Rapid acquisition programs (Middle Tier of Acquisition – MTA) and low-cost attritable systems achieve functionality using leading-edge COTS components vetted by prime vendors



Major Capability Acquisition



Middle Tier of Acquisition

3. Pilot Programs Highlight Scalability Issues with MQA

- Data generated for MQA has an undefined format, is massive in volume and predominantly manually generated
- JFAC currently performs a key role with all RAMP performers; it is unclear how this will scale with future engagements (ideas were provided by T&AM team)
- Mitigations defined by MQA are not aligned with commercial best practices and are often vague, requiring customization and clarification on a per-performer basis
  - This drives costs to individual programs, likely beyond available resources
  - Also reduces incentive for companies to take part in MQA
- RAMP participants spent a significant amount of time clarifying and collecting the data required by the government, and expect a financial incentive to do so

Recommendations for Future Foundry Interactions

- Clarify details regarding roles, responsibilities, and the expected sequence of events entailing the MQA process – opportunity for standardization
- Consider examining the data from RAMP performers and determine any commonalities that could be used to help define mitigation requirements and format – opportunities for standardization and automation across foundries
- Identify opportunities to better align MQA with commercial best practices
- Strive to provide more explicit written guidance to performers on mitigation intent
- Consider explanatory NDA guidance to performers to develop a common NDA framework and speed up NDA establishment; will need to include NDA establishment in all acquisition and contracting processes that touch MQA
- Work with industry to establish the intent and acceptable data artifacts for use of 3rd-party IP (3PIP) providers

4. Impacts to Capability, Cost, and Schedule

- Many stakeholders professed that access to state-of-the-art custom microelectronics would be critical, but few (1-2) described a specific need for leading edge (i.e., 14 nm or better)
- Cost and schedule options likely to expand with greater adoption of continuous lifecycle improvement techniques, e.g., MOSA
  - However, MQA does not address the fact that state-of-the-art custom microelectronics fabrication is 10X the cost of more mature technology nodes
- Vetting of COTS options is likely to become even more essential with proliferation of “chiplets”
  - Chiplets are small semiconductor dies that can be integrated heterogeneously with a larger compute platform – see the SHIP program, for example
  - MQA does not address chiplet assurance other than as CIC components
  - Instead, chiplets should be assessed as fungible hardware IP

Capability and Cost Impacts of MQA Were Difficult to Compare Against Other Approaches

- No direct 1-1 comparisons available of a chip fabricated using MQA alongside the same chip targeted at a Trusted Foundry
- RAMP pilot fabricators would not release costing of MQA mitigations, even under NDA
- DMEA was asked to provide metrics for Trusted Foundry accreditation so that a comparative assessment could be conducted
  – DMEA stated that Trusted Foundry and MQA were not comparable, and no data were provided
- DIB fab facility operators commented that engaging in MQA would add costs since new business processes and architectures would have to be built – these would be passed to USG

Finding: We were not able to carry out an assessment of cost impact to programs of implementing MQA due to a lack of data from DMEA and manufacturers

Recommendation: DoD should conduct a cost assessment of MQA contracting with the necessary private sector entities to obtain costing data

5A. Stakeholder Key Findings – US Government

MQA Technical and Implementation Findings

- MQA addresses limited threats, focusing on fabrication facility – doesn't address threats existing outside of fab and other aspects such as reliability and fielded assurance
- Awareness and knowledge of MQA varied significantly across the DoD/IC stakeholders we interviewed
  - Most had heard of MQA but didn't know specifics of how it worked
  - Several had not heard about JFAC at all
- Stakeholders with great deal of familiarity with MQA felt it wasn't mature enough (yet) to be implementable by a program
- Only one stakeholder supported DoD programs that had put MQA into practice; several more were considering doing so
  - One program had successfully implemented LOA1 and was actively working LOA2

Other Findings

- JFAC support may be enhanced by incorporating mature assurance processes/capabilities from other agencies (e.g. MDA)
  - JFAC consultation process may not be repeatable – might get a different answer if asking a question earlier or later
  - JFAC lacks resources to help all the programs that could benefit from MQA
- FPGAs and CICs are considered as critical components in many programs – therefore tolerance of mission risk is low
  - MQA does not support calculation of overall risk to mission (mission risk is conditional on ME threat likelihood and MQA does not quantify this)
- Extent and quality of assurance efforts vary greatly between programs (personnel-dependent) based on information collected during interviews

USG Stakeholders – Additional Findings

- DoD MQA team has not fully explored existing processes and best practices currently in use within the DoD and the microelectronics community at large
- MQA documentation does not reflect detailed understanding of the nuanced and complex dependencies among the contributors to the chip design and fabrication process – especially as relates to the supply chain as a whole
- MQA process is currently not well communicated across the relevant organizations within the DoD: documents remain in draft, are incomplete and limited distribution

5B. Stakeholder Key Findings – Commercial Industry

- Strategies adopted by commercial industry to ensure the security and integrity of their products are compatible with the proposed MQA approach
- Commercial companies are generally aware of security concerns and challenges of supply chains but follow different paths to the security and assurance of their hardware products; this includes standards, best practices, trade secrets, and cycles of innovation
- Microelectronics production supply chains are global, complex, and present difficulties for perfecting assurance
- With commercial companies, the motivation for market growth and profits drive the innovations needed for product/service/industrial competitiveness and are considerations during project decisions

Recommendations from Commercial Stakeholders

- Develop training for program managers in implementation of MQA and increase outreach efforts to communicate and educate industry on MQA details
- Engage with standards development organizations to adopt all or components of MQA; update contracting to require these standards for covered microelectronics
- Study the cost of implementing MQA and develop a plan to address and continuously reduce the highest cost elements, such as more extensive use of digital twins and equivalency checking. The pilot efforts are likely to provide much of the initial estimation of cost and burden; independent analysis useful for confirmation
- Study the residual risks especially in complex use cases; develop approaches and methods for consequence management
- Study private sector capabilities for supply chain illumination/intelligence, and independent validation and verification testing; understand the raw capabilities and the ability to scale up in some fashion from Government internal tools like AMARO and the JFAC's capabilities to give programs (and contractors/suppliers) more options

Other Top-Level Observations

- MQA is an R&D effort in continual progress
  - MQA version 4.5/5.0 is under development now
  - Version 4.0 was the subject of this assessment
  - Pilot activities that were assessed used Version 3.0
- The areas of most significant concern (COTS, LoA 3) are least specified and were not suitably completed for review during this assessment
  - MQA is expected to cover multiple dimensions, e.g., assurance (LoA 1-3) and component type (CIC vs. FPGA vs. COTS)
  - Only CIC and FPGA at LoA 1 were ready for assessment (FPGA LoA 2 is in draft)

Conclusions

- MQA represents a good-faith standards and practices initial/partial technical solution to provide ME sourcing flexibility to DoD targeting Congressional and DoD intent
- MQA is <u>not ready for deployment</u> in present form, but could be made to work
- Significant gaps exist rendering MQA <u>an incomplete solution</u> for addressing threats
  - Especially outside the design-to-production window
  - Coupling to mission contexts is ambiguous and underspecified
- Focused near-term attention and investment are needed to ensure:
  - Sufficient alignment with Service/Component acquisition and sustainment pathways
  - Cogent communication and training on MQA – <u>critical gap</u> blocking adoption by Services, Components, and private industry, many of whom are completely unfamiliar with MQA
  - Efficient multilateral collaboration between DoD and industry participants, especially with respect to intellectual property (IP) and non-disclosure agreements (NDAs)
  - Timeliness of MQA completion so that it can be used when relevant commercial capabilities come online, e.g., via RAMP-C and CHIPS Act investments

Recommended Next Steps

- Implement the technical recommendations associated with each of the Key Findings
- Continue to promote the evaluation of MQA in pilot programs
- Continue to monitor and assess iterated evolutions of MQA and in-stream pilot artifacts
- Assess MQA use cases being articulated in forthcoming OUSD(R&E) white papers
- Conduct comparative evaluation of MQA with alternatives under development (e.g., by the Air Force and by academic institutions)
- Assess efficacy of any remediations and modifications to be put in place by OUSD(R&E) in response to recommendations of the Independent Assessment Team

Team Composition

MITRE

- Shamik Das
- Mike Anderson
- Krystin Baker
- Lisa Bembenick
- Greg Cardinale
- Roberto Landrau
- Eric Lautenschlager
- Isaac Matthews
- Brett Meadows
- Richard Potember
- Sean Ricks
- Jim Wall

MIT Lincoln Laboratory

- Brendon Chetwynd
- Bob Atkins
- Jonathan Bernays
- Chris Connelly
- Kyle Ingols
- Brendan Mulholland

Sandia National Laboratory

- Vivian Kammler
- Yalin Hu
- Keith Vanderveen
- Keenan Harris
- Kenneth Hayes
- Eric Vugrin
- Greg Wyss

Draper

- Geremy Freifeld
- Marjorie Quant
- Joshua Krause
- Eric Leveille

GTRI

- Tom McNeil
- Lee Lerner
- Chris Clark
- Chris Coen
- Bill Hunter
- Robert Lingle
- Nelson Lourenco
- Brent Wagner
- Ben Yang

Appendix:
Detailed Exposition of Findings

Key Questions and Index to Answers

- What is MQA? i.e., provide an unbiased definition/specification of MQA, provide a statement of what was intended by Congress via legislation, and assess what capabilities and components MQA is intended to incorporate or enable.

  Addressed in main briefing. [link]

- What are the specific needs that MQA is addressing and what will not be addressed? If a need is not addressed by MQA, is there an existing mechanism to address that need or is there a gap?

  The Key Findings in the main briefing speak to the needs unaddressed by MQA and the Recommendations propose mechanisms to address these needs.

- Can the proposed MQA framework and methodology provide DoD with the equivalent of assured access to trusted microelectronics? Will MQA enable the DoD to obtain levels of security, assurance, and/or program protection exceeding that provided via the Trusted Foundry model?

  The MQA definition has evolved over time and now includes components of the Trusted Foundry model as means to satisfy MQA. Therefore, the answer to this question technically is 'yes'. However, a direct comparison was attempted between the Trusted Foundry model and the non-Trusted Foundry aspects of MQA. This was not possible due to a lack of required data. [link]

- Will MQA provide programs with microelectronics whose performance (e.g., speed, power, other application-specific figures of merit) exceeds that available via existing Trusted Foundry capability, and if so, to what extent (i.e., can the increase in available performance be quantified)? What will be the resulting system performance impact to weapon systems?

  Program development and fielding cycles vary widely and for major capability acquisitions, the timeline greatly exceeds the evolutionary lifetime of state-of-the-art microelectronics. MQA possibly can reduce, but will not eliminate, this bottleneck. Therefore, these major programs might gain access to newer, but not state-of-the-art, technology. In contrast, rapid-prototyping programs for subsystem capabilities might be executed on a faster cadence and might therefore improve performance using MQA. However, MQA needs further tailoring and streamlining in order not to burden such programs with significant cost and schedule impacts. [link]

  PEOs that were consulted for this assessment professed that they would use state-of-the-art microelectronics if available (in other words, that "no one would say no" to having access to that technology) but also that if trading off higher performance vs. higher mission assurance, they would always choose in favor of mission assurance. [link]

Key Questions and Index to Answers (cont'd)

- Does MQA put forward a set of standards that meet the requirements and intent of the 2020 NDAA Section 224?

  Partially, yes. [link]

- Are the MQA tools and standards compatible with industry supplier practices, such that multiple suppliers at the state of the art are expected to engage with DoD using the MQA framework so as to be available for sourcing of components? What measures will be put in place to ensure or monitor industry compliance with agreed-upon standards?

  Partially, yes. The standards are tabulated as commercially compatible best practices, in keeping with Sec. 224. There are unaddressed gaps with respect to the cost to suppliers of implementing MQA standards or mitigations, and no mechanisms for compliance certification or qualification. [Documented in findings throughout the briefing and appendix.]

- Does the proposed MQA approach take advantage of or work compatibly with similar practices adopted already by commercial industry to ensure the security and integrity of their products?
  - What practices does industry implement to achieve security (confidentiality, integrity, availability) in their products? Do commercial manufacturers have any quantitative measures they customarily apply?
  - What commercial standards exist currently in this space that are industry-originated and/or widely adopted or respected by commercial suppliers?

  Proposed standards are generally compatible with industry practices and commercial stakeholders stated that many of these practices are already commercially adopted. [link] However, stakeholders also stated that some proposed MQA mitigations are not aligned with commercial practices to address the relevant threats. [Further details are in this appendix, e.g., this link.]

- What is the role/charter of JFAC as relates to executing the MQA methodology? If that role/charter is not clearly defined, what is required?

  JFAC's role is not clearly defined. There are expectations by many stakeholders that JFAC would fulfill a technical authority role with respect to execution of MQA. The MQA authors intend for JFAC to be one option among several to be identified by Programs or Services. While JFAC is available for consultation, no entity has been designated with the authority to certify compliance with MQA. [link]

Outline of Detailed Exposition of Findings

- Technical Evaluation of Attack-Tree Countermeasure Analysis
- Assessment of Pilot Program Activities
- Stakeholder Engagement and Perspectives

ACMA Evaluation Scope

According to “Microelectronics Quantifiable Assurance (MQA) Independent Assessment: Terms of Reference”, “the MQA Independent assessment will address … An evaluation of the MQA’s Attack-tree Countermeasure Analysis (ACMA) methodology for its viability in assessing risk and identifying mitigations.”

Focus was on reviewing the documents provided in the MQA Rev 4.0A package to

- Gain an understanding of the MQA process
- Gain an understanding of the ACMA framework
- Gain an understanding of the relationship between MQA, ACMA, and the Microelectronics Assurance Framework (MAF)
- Gain an understanding of how risk is assessed, evaluated, and quantified under the ACMA framework
- Identify potential limitations or issues with MQA and the ACMA framework.

ACMA Evaluation Process

The process used for evaluation of the ACMA materials is described below:

1. Assess whether the mitigations listed for each threat for custom integrated circuits (CIC) and field-programmable gate arrays (FPGAs) are effective.
2. Assess whether the mitigations definitions are complete, coherent, and can be implemented by programs.
3. Rank the threats by importance in providing assurance.
4. Perform a gap analysis on the ACMA materials as delivered (documents revision 4.0A).
5. Craft recommendations for improvements and coverage for identified gaps.

ACMA Evaluation Findings

The four major findings of the ACMA Analysis are:

1. Significant gaps exist in the current ACMA implementation for some of the CIC and FPGA threat scenarios.
2. Definition of several mitigations do not provide sufficient detail to enable effective program implementation and, as a result, may lead to unexpected and unacceptably large residual risks.
3. ACMA process and implementation provide insufficient guidance for risk and residual risk quantification.
4. The differentiation of the defined threats between the Level of Assurances (LoAs) is not sufficiently defined.

ACMA Evaluation Finding #1

Significant gaps exist in the current ACMA implementation for both CIC and FPGA threat scenarios.

The team first assessed whether the threats were successfully allayed by the mitigations the MQA documents assigned to each threat. This assessment assigned a stoplight color to each threat. Ratings are defined as follows:

- A Green rating indicates that the assigned mitigations should be successful in allaying the threat.
- A Yellow rating indicates that
  a. Some risk may remain even if the listed mitigations are implemented. Or,
  b. The mitigations & associated data products listed for the threat are insufficiently defined and, thus, may make effective implementation of the mitigation challenging.
- A Red rating indicates that the threat would not successfully be allayed by the assigned mitigations & data products.

Following the stoplight assessment of the threats and mitigations, the team ranked the threat scenarios according to *severity tiers*. These tiers are defined as follows:

1. A **tier 1** (Red) threat would compromise the CIC or FPGA design or manufacture under the assumption that effective mitigations are not in place [see note].
2. A **tier 2** (Yellow) threat would not directly compromise the design or manufacture under the assumption that effective mitigations are not in place [see note]. However, the threat could result in severe cost, schedule, and performance issues for the program. The program may deploy deficient components and dispose of good components.
3. A **tier 3** threat would not compromise the design or manufacture of the component, but an adversary can gain design information that may be used to compromise the component or weapon system in the future.
4. A **tier 4** threat would not compromise the design, manufacture, or specific design data.

Custom Integrated Circuit (CIC) Threat Tier vs. Stoplight Rating	Red – Threat Not Mitigated	Yellow – Partial Mitigation	Green – Threat Mitigated
Tier 1 – Direct Component Compromise	**2**	**10**	4
Tier 2 – Significant Programmatic Effect	**3**	**2**	0
Tier 3 – Design Data Leakage	0	5	4
Tier 4 – No Component Compromise or Design Data Leakage	2	0	2

Field Programmable Gate Array (FPGA) Threat Tier vs. Stoplight Rating	Red – Threat Not Mitigated	Yellow – Partial Mitigation	Green – Threat Mitigated
Tier 1 – Direct Component Compromise	**1**	**6**	5
Tier 2 – Significant Programmatic Effect	**1**	**3**	0
Tier 3 – Design Data Leakage	0	0	0
Tier 4 – No Component Compromise or Design Data Leakage	0	0	0

ACMA Evaluation Finding #2

ACMA mitigations are insufficiently defined.

Several mitigation definitions are either vague, undefined, or could be improved through additional specification or reference to guiding standards. The team asses that

- 12/61 (20%) FPGA mitigation definitions could be improved.
- 17/88 (19%) CIC mitigation definition mitigations could be improved.

In the case of CIC, Post Silicon Mitigation seems to be the predominate factor in providing data to successfully mitigate several tier 1 and tier 2 threats. Post silicon mitigations data requirements are not defined in sufficient detail for implementation. Post silicon mitigations require significant cost and schedule investment from the program, and this investment may not be apparent at the outset of MQA implementation.

In the case of FPGAs, the ACMA implementation does not account for field updates. Mitigations specified for initial factory provisioning may not be practical for urgent fixes during deployment.

ACMA Evaluation Finding #3

The ACMA process and implementation provide insufficient guidance for residual risk quantification.

The ACMA process is not sufficiently detailed regarding residual risk quantification in the information provided. Appendix B of “DoD Microelectronics Assurance Framework” (Volume 1) generally describes the elements and methodology, but it lacks information describing how risk is evaluated and quantified under the ACMA. In particular,

- This document indicates that “each branch of the ACMA tree ends in a residual risk” and “acceptable risk depends on the LOA.” However, the document provides no indication of how the risk determination is done. It is even unclear whether the risk in ACMA is qualitative, semiquantitative, or fully quantitative, and no further reference is indicated.
- Information describing what a “program-specific risk profile” includes is insufficient, and no further reference is indicated.
- Description of what constitutes “acceptable residual risk” and the manner for comparing “residual risk” and “acceptable residual risk” is insufficient, and no further reference is indicated.
- The process for evaluating and quantifying residual risk and residual risk is insufficient. The most specific statements the team found regarding risk evaluation appear in the presentation from the Independent Assessment Teams Kickoff Meeting. On Slide 16: “The Joint Federated Assurance Centers (JFAC) can provide threat specific risk evaluation.” References to “RIO, TSN, ACMA, FMEA, and others” as risk assessment methods (from Slide 58), when examined, do not provide sufficient detail. Specifically, RIO and TSN describe only a basic generic risk assessment process of "identify risks" and "estimate likelihood", with no indication as to how those tasks should be done, or the results verified and validated in a cybersecurity context. FMEA is a similarly generic methodology, and ACMA provides no additional guidance.

ACMA Evaluation Finding #4

Differentiation of defined threats between Levels of Assurance (LoAs) are undefined.

The assessment team reviewed the definitions of the Level of Assurances with the government team and came to an understanding of definitions at the final component level. However, discussions and questions on how to separate the identified threats by LoA were largely inconclusive.

The assessment team received documentation on threats and mitigations for LoA 1 for both CIC and FPGA, and preliminary documentation on FPGA LoA 2. No LoA 3 information or LoA 2 information for CIC was provided.

Without associated documentation for LoA 2 and LoA 3 implementations, it is not possible to grade the total threat-space of vulnerabilities. The ACMA subtask assessment plan originally called for an independent derivation of the threat-space for FPGA and CIC, but this task is not practical without a clear delineation between the LoA threat-spaces.

Other ACMA Evaluation Findings

- As adversary capabilities evolve and threat intelligence continues, it is possible (and likely) that the ACMA framework will need to consider additional threat scenarios and mitigations. The documentation provided does not describe a process for updating the ACMA framework in the future and to ensure that it is up-to-date. This omission may pose future challenges and lead to potential vulnerabilities and increased, unrecognized risks.

- The specific threat vector for obtaining access (insider or network intrusion) is not specified in most FPGA scenarios. As a result, scenarios which do not specify the threat vector may not be fully mitigating against it.

- There are notable inconsistencies between the CIC and FPGA spreadsheets. For example, the same mitigation is sometimes defined differently in the 2 spreadsheets. Additionally, some inconsistencies exist between the Word documents and Excel spreadsheets

ACMA Evaluation Recommendations

1. The department should invest in a robust Post Silicon Mitigation ecosystem that can be used for the entire department, including several major programs executing concurrently at different classification levels. If these mitigations negatively affect program schedules, they will likely be bypassed.
2. The ACMA should be updated to address and articulate threats and mitigations that account for field updates of FPGAs.
3. The ACMA should expand upon the mitigation descriptions and ensure that they are clearly defined, provide sufficient guidance on actions to take, and provide exemplars of data products associated with each and every mitigation.
4. MQA needs to articulate a strategy for quantifying residual risk in the event that one or more mitigations are not able to be fully implemented by programs.
5. A process should be articulated, and a regular cadence should be adopted, for the incorporation of threats and mitigations into the current and future ACMA implementations.
6. Effort should be made to ensure the CIC and FPGA implementations are consistent across the documentation.

Outline of Detailed Exposition of Findings

- Technical Evaluation of Attack-Tree Countermeasure Analysis
- Assessment of Pilot Program Activities
- Stakeholder Engagement and Perspectives

Scope of Pilot Program Assessment Work

Evaluate data and evidence being generated by RAMP, RAMP-C, and SHIP pilot programs to demonstrate the viability of the MQA method

- Evidence will include but is not limited to technical performance of the microelectronics being fabricated via these pilots, in comparison with leading-edge commercial off-the-shelf capabilities for general-purpose and special-purpose microelectronics.
- This evaluation will include assessment of impacts/mitigations should the data be unavailable or insufficient to execute the MQA methodology as intended

High-Level Approach

- Engagement focused on RAMP program based on performer availability
- Performed introductory interviews with most RAMP performers
- Engagement scope varied per performer, but notable engagements included:
  - Microsoft, Intel and GlobalFoundries met with the IAT numerous times over the course of the assessment. These organizations provided detailed briefs in response to the IAT's questions
  - In depth engagement with other performers constrained by NDAs – assessments were conducted by the IAT subteams that were able to put NDAs in place

Pilot Program Finding #1

- Feedback on MQA mitigations have not been consistently communicated to RAMP performers; It is unclear how the effectiveness of MQA will be evaluated post-deployment
  - Explicit guidance needs to be provided to MQA implementors on feedback mechanism between them and the appropriate govt. organizations
  - JFAC currently performs a key role with all RAMP performers; it is unclear how this will scale with future engagements
  - Some of the details of roles and responsibilities are not clear in MQA; ambiguity exists as to what is expected of a performer post assessment and how to address unacceptable risk determinations
- Recommendation: clarify details regarding roles, responsibilities, and the expected sequence of events entailing the MQA process

Pilot Program Finding #2

- MQA generated data consistently contains proprietary information and thus cannot be easily shared between vendors, performers, and across programs
  - A majority of RAMP performers stated that the number of NDAs required to deliver information dramatically exceeded expectations
  - Some information (e.g., personnel practices) was considered trade secrets by RAMP performers, and would not be shared regardless of NDA status
  - In several cases, the third-party IP (3PIP) providers did not want specific information shared with the government (e.g., Country of Origin)
  - Following completion of an MQA assessment, it is unclear how residual data will be handled and how that data will be used to inform lessons learned and improve the process
- Recommendation
  - Consider explanatory NDA guidance to performers to develop a common NDA framework and speed up NDA establishment; Include MQA NDA establishment in contracting processes
  - Work with performers to establish the intent and acceptable data artifacts for use of 3PIP providers

Pilot Program Finding #3

- Data generated for MQA has an undefined format, is massive in volume and predominantly manually generated
  - In the absence of a standardized format, many RAMP performers delivered data based on their preferences
  - The amount of data generated is very large, and that the opportunities and incentives to automate this process are unclear
  - These two factors create a scalability challenge in processing of the data by third parties to validate mitigation compliance
- Recommendation
  - Consider examining the data from RAMP performers and determine any commonalities that could be used to help define mitigation requirements and format
  - Work with foundries to identify and incentivize automation opportunities

Pilot Program Finding #4

- Mitigations defined by MQA are not aligned with commercial best practices and are often unclear, requiring clarification on a per-performer basis
  - Several RAMP performers mentioned that the mitigations did not fall in line with their company practices
  - One performer pointed out that the data requirements for the mitigation were high level and vague
  - Another performer stated they spent thousands of hours in discussions with the government to clarify the intent and level of detail required to meet the intent.
  - The lack of clarity and alignment with the commercial sector is causing the performers to submit partial data or sometimes waive entire mitigations.
- Recommendation
  - Identify opportunities to better align MQA with commercial best practices
  - Strive to provide more explicit guidance to performers on mitigation intent

Pilot Program Finding #5: Cost

- RAMP participants spent a significant amount of time clarifying and collecting the data required by the government, and expect an incentive to do so
  - One participant stated that the initial cost to automate their processes to line up with MQA would cost 7-8 figures, with subsequent programs costing somewhat less.
  - Another participant noted that if MQA was not required, it will not be budgeted for in order to keep cost competitive.
  - Initial costs to implement MQA is large.
  - Combined with the data requirements findings (large amounts of non-normalized data) creates a large scale, manual process that will incur significant cost.
- Recommendation
  - Determine a method to allow data re-use across programs for 3PIP.
  - Focus efforts on normalizing data requirements and process automation.

Outline of Detailed Exposition of Findings

- Technical Evaluation of Attack-Tree Countermeasure Analysis
- Assessment of Pilot Program Activities
- Stakeholder Engagement and Perspectives
  - U.S. Government Stakeholders
  - Commercial Stakeholders

USG Stakeholder Assessment Goal and Approach

- Awareness of MQA
- Awareness of other existing frameworks and tools
- Current practice/policies for microelectronics assurance, including supply chain risk analysis
- Willingness to implement MQA
- Challenges to implement MQA

USG Stakeholder Key Findings

- Awareness, knowledge of MQA varied significantly across the DoD/IC stakeholders we interviewed
  - Most had heard of MQA but didn't know specifics of how it worked
  - Several had not heard about JFAC at all
- JFAC support may be enhanced by incorporating mature assurance processes/capabilities from other agencies (e.g. MDA)
  - JFAC consultation process may not be repeatable – might get a different answer if ask a question earlier or later
  - JFAC lacks resources to help all the programs that could benefit from MQA
- FPGAs and CICs are considered as critical components in many programs – therefore tolerance of mission risk is low
  - MQA does not assess risk to <u>mission</u>
- MQA addresses limited threats, focusing on fabrication facility – doesn't address threats existing outside of fab and other aspects such as reliability and fielded assurance
- Extent and quality of assurance efforts vary greatly between programs (personnel-dependent) based on information collected during interviews
- Only one stakeholder supported DoD programs that had put MQA into practice; several more were considering doing so
  - One program (executed by SNL for DoD) had successfully implemented LOA1 and was actively working LOA2
- Stakeholders with great deal of familiarity with MQA felt it wasn't mature enough (yet) to be implementable by a program

USG Stakeholder Additional Findings

- MQA fits (or must fit) into a large body of security/assurance processes acquisition programs expected to follow, or follow as best practices, involving microelectronics, software, other components
  - Existing security/assurance practices serve a variety of objectives, from enabling foreign military sales to preventing sabotage
  - Not clear how all of these security/assurance practices relate or should relate
  - Stakeholders expressed desire for integrated assurance process – not just processes for part of supply chain (like MQA), but true multi-disciplinary, system-level process (of which microelectronics is one aspect)
- Programs and agency stakeholders interviewed almost all said they were understaffed in their assurance efforts – not sure how they would find the staff time to learn MQA
- Many stakeholders felt MQA not mature enough to be implementable (yet) – standards documents still in too much flux
- Connection between metrics collected through MQA and “assurance” not well defined/specified

USG Stakeholder Additional Findings (cont'd)

- LoA definitions vague, subject to (differing) interpretation by programs
- Some agencies (e.g. MDA) have very mature assurance processes/capabilities – MQA could be improved by incorporating some of these
- Possible implementation of MQA by programs likely to be ad hoc, highly specific to each program
- Agencies with mature assurance processes should also be asked to evaluate MQA for compatibility/synergy with their existing processes
- Some programs/agencies using guidance from other sources (e.g. NIST 800-161) to manage supply chain risk
- One stakeholder believed MQA should be executed by the prime contractor, with the prime then explaining to the program and MDA why they had confidence in the chips vetted through the MQA process
- One stakeholder expressed confusion about how MQA would fit into existing security practices/processes for weapons/platform acquisition, for example how would it work with anti-tamper?

Key Quotes from USG Stakeholders

- **Service Acquisition Executive**
  - "I don't know who would answer 'no' to that" (answering the question of their need for state-of-the-art microelectronics)
  - We need a tailored approach since programs run the full breadth and there's no need to do the same thing for every program
  - It can get onerous to add so much burden to programs when the Program Manager has not assessed risks

- **Navy Program Office**
  - Most programs need state of the art microelectronics
  - A subset of programs currently do not have their application specific integrated circuits (ASICs) needs met and would benefit from expanded technology offerings under MQA
  - MQA would be a comprehensive solution, but it is too early to say that any program will fully adopt it. Many programs already have assurance procedures they feel confident in and would like to continue using them; MQA principles would likely be utilized in specific scenarios such as vetting soft IP
  - Determining the ultimate role for the Joint Federated Assurance Center (JFAC) in MQA will be crucial

- **USAF PEO**
  - Avoid point solutions by platform, trying to move away from that; enterprise solutions are being sought
  - Policy needs to reflect ability to export platforms
  - Policy that creates moving targets for performers that oversee multiyear acquisition cycles can make things difficult for programs
  - JFAC Levels of Assurance are seen as more as a compliance issue than a design issue

Key Quotes from USG Stakeholders (cont'd)

- **Navy Program Office**
  - Programs have COTS microelectronics, GOTS, SOA, custom, … everything
  - We do quality assurance on almost everything
  - Want assurance the microelectronic parts are good but in some applications like arrays can still operate
  - Who owns the system-of-systems; how do you get ownership of levels of assurance at the system of system level?
  - A successful new policy would be clear in its directives to the program, and also provide enough resources for programs to staff and train the number of personnel actually needed to implement the policy as it was intended.
  - They have already adopted some aspects of MQA to mitigate risk in their systems

- **NNSA**
  - The program anticipates that it will need to incorporate some microelectronic components that not available under the current procurement guidelines, with custom integrated circuits (CICs) being the highest priority for the program. MQA would be a benefit for this
  - Likely to implement MQA in some form within the program
  - The program would like to work with DoD to understand which portions of MQA really reduce their residual risk on a single mitigation or measurement-by-measurement level
  - An ideal situation would be adding a few key portions of MQA for maximum impact instead of broad adoption

Further Observations and Feedback

Department of the Air Force – 26 October 2022

- MQA is not well defined – unstable draft documentation over several years and still incomplete.
  - MQA as communicated seems to focus primarily on the fabrication facility (foundry) and does not address wider range of vulnerabilities (e.g. 3rd party IP, OSAT and PCBs).
  - While ACMA recognizes other threat vectors, risks outside the fab (e.g. packaging) are not fully addressed in current draft process.
  - ACMA is incomplete in that it does not properly include adversary capabilities and intent.
  - Hard to accurately estimate resources and schedule for implementation.
  - Significant aspects of what the MQA process needs to be reside outside of the foundry.
  - Incentives do not align between chip maker and chip customer.
    - Cost Benefit analysis over the life-cycle of the system.
    - Implementation of MQA may be viewed as detrimental to business interests by 3rd party suppliers.
  - Chip maker lacks the full design access and incentive to assure the integrity of 3rd Party IP.
  - Difficult to scale results for MQA from RAMP.
    - RAMP pilot does not scale due to manual processes and incomplete implementations.
    - “People are grading their own homework” – lacks independence – zero trust principles not really implemented.
  - Feedback is that Government (specifically JFAC as currently formulated) lacks sufficient expertise to conduct full evaluation of relevant mission risks.
  - JFAC may not give repeatable feedback (SME dependent)
  - Levels of Assurance are very subjective with no methodology to translate into objective measures.
  - Program managers drive the type of ACMA – ad hoc process at this point.

Further Observations and Feedback (cont'd)

Department of the Air Force – 26 October 2022

- Wider acquisition community and commercial industry not informed of MQA objectives and vision.
  - Voice of those responsible for implementation is not represented in the draft process.
  - Industry input neither solicited nor accepted.
- Education and outreach – Government has not described all opportunities for compromise throughout the supply chain nor delegated responsibilities for each of the opportunities.
  - Detail each opportunity.
  - Responsible party for each step.
- In its current form, MQA is not seen as mature, feasible or helpful.
  - Work remains to capture and incorporate broader input.
  - Outreach and education across the supplier and acquisition communities.

Further Observations and Feedback

Missile Defense Agency (MDA) – 17 November 2022

- MDA has an existing process wherein every "logic bearing device" is reviewed.
  - Significant work has been done in this area, but the MQA team did not reach out to MDA.
  - MDA unfamiliar with MQA and there is no record of any engagement by the MQA team with MDA.
  - MDA process addresses quality, supply chain risk management (SCRM) and counter-intelligence.
  - MDA assesses risk and part criticality at high, medium and low. High and Medium risk require mitigation or re-design. Low risk is accepted due to resource constraints.
- MDA Industrial Manufacturing Group monitors large programs of record with goal of near-continuous monitoring of supply chain.
  - Developing AI/ML tools to enable supply chain data monitoring and reduce human in the loop processes.
  - Beginning to consider outreach to other DoD entities to discuss tool integration.
- Significant backlog of parts to review due to understaffing results requires prioritization of most critical parts and risk acceptance.
  - "Risk Board" determines if risk is too high and can direct a re-design or other mitigation.
  - QS recommended a follow on discussion with DEI (Technical Intelligence) and MDA Counter-intelligence.

Further Observations and Feedback

MDA – 1 December 2022

- MDA QS initiates an RFI on logic bearing devices identified in program protection plans.
  - Starts with program via criticality analysis identifying logic bearing devices (Category 1 and 2) as specified in MDA 5200.08.
  - System level to component traceability.
- MDA has existing Supply Chain and Cyber Risk Management organization and process.
  - Performs security and intelligence reviews of category 1 and 2 critical components.
  - Strictly limit assessment to risk and vulnerabilities within the supply chain, external threats to supply chain.
- Cyber-SCRM (C-SCRM) element reviews the component from technical engineering perspective, specifically looking for threats.
  - Considers foreign intelligence threats to the component.
  - Considers cybersecurity / cyber threat intelligence.
- Program Offices have an Engineering Review Board that evaluate overall risk.
  - Programs assesses risk, compiles it into a package that is then brought up to the appropriate level for review and adjudication.
  - If risk is high enough, then it will go up to the Agency's Chief Engineer for final adjudication.
- Effort is under-resourced/under-staffed so only higher risk components can be evaluated.
  - Resources "desperately needed" – far too many RFI's for the number of analysts available.
  - COTS and lower risk components can not be evaluated with current resourcing.
  - AI and ML tool being developed may help but expert analysis and Program Manager are still required to make a decision.
- Inefficiencies due to lack of information sharing across programs and organizations.
  - Opportunity for collaboration across organizations and programs.
  - Policy limits information / intelligence sharing.

Further Observations and Feedback

US ARMY – 14 December 2022

- SMDC is a major operator of system-of-systems yet has no input to risk assessments or judgement on criticality of individual systems to systems-of-systems performance.
  - SMDC Technical Center involved in testing, future concept development and prototyping including directed energy systems.
  - Reorganizations driving a lot of change in responsibilities (US Space Force and Army Futures Command).
  - Observed the Army might be the biggest users of ME chips, since every soldier likely has chips in his hands.
- Concerned if DoD is broadly assuring we use secure microelectronics as we develop and deploy Artificial Intelligence.
  - Capability is priority but no clear line between defense and commercial - "when they buy a computer, they buy a computer for example".
  - At some point, someone needs to "herd the cats, get all the services represented".
  - "Nobody has the money to do it all"; must address across all of DoD / USGOV (e.g. NASA is a "major partner" of SMDC)
  - Look where the greatest risks/benefits are…enforce safe/cyber-secure processes (e.g. foundries).
- SMDC current process is to perform system level checks on delivered capabilities.
  - SMDC does not address ME component or subsystem level checks.
  - Recognize there will be great risk going forward for Army with complex systems-of-systems like ground-based missile defense.
  - Reliant upon MDA that provides the Ground-Based Interceptors to SMDC to have gone through the process at the component level.
  - SMDC must have reliable and safe access to microchips for multi-domain operations (MDO) of the future.

"As we pursue this in policy, it is a whole different ballgame to make microelectronics that work in wars"

Further Observations and Feedback

US Navy – 15 December 2022

- PMA-213 and SPN-35E Program Office not informed or familiar with proposed MQA process prior to interview.
- SPN-35E program works with cyber counterparts in the Navy to vet components and sources for this program.
  - Silicon Expert vet FPGAs but it's a hard to perform "deep dive" vetting for some components.
  - Receive FPGAs from the Philippines that are covered by open trade agreements, but it is difficult to make sure we have approved vendors to purchase from (i.e., Trusted Foundry).
- "Very competent people" within Navy and contractors so expectation that those responsible for a piece of hardware/software are taking risk mitigation into consideration.
  - Flowing responsibility down to selected contractors and trusting them.
  - RMF focus applied to systems in terms of confidentiality, integrity, and availability.
  - Following NIST guidance – whatever NIST says to look at, those are the controls applied to the system.
  - All program aspects rolled into one risk: configuration management, system components, documents, programmatic information, etc.
  - Ad hoc information sharing based on the right expert being at meetings and bringing up issues.
- Program office has Science and Intelligence Liaison Officer (SILO) who is go to person for Counter-Intel.
  - Lead time on some parts (70 weeks or more) has resulted in program timeline versus supplier sourcing risk trades.
  - SILO helps evaluate list of needed parts to find alternative but issues greater than resources available.
- ME supply chain causing NAVAIR significant schedule and budget issues in replacing obsolescent systems in Fleet.
  - SPN-35E is taking a different approach to improve visibility wherein program office serves as the prime and lead systems integrator.
  - Program office maintains total system responsibility while using UARC as technical resource to address internal technical resource constraints (i.e. NAVAIR Manufacturing and Quality has only 70 people to support all NAVAIR programs).

Further Observations and Feedback

Defense Microelectronics Advisory Group (DMAG) – 4 January 2023

- DMAG tasked by OUSD(RE), Dr. Shenoy, to provide a "collective view" of MQA made four major recommendations:
  - Tightly couple future MQA policy iterations to assist assurance, expanding beyond integrated circuit components.
  - Align DoD MQA strategy with commercial best practices to produce scientifically rigorous quantitative test analysis and statistics.
  - Organization analogous to Anti-Tamper Executive Agent to administer MAF to specifically implement/oversee the operational MQA effort.
  - Leverage commercial certification methodology with MQA standards to develop quantitative requirements – specifications/Figures of Merit.
- Very important for MQA to have a tight definition of what the metrology is attempting to provide.
  - Objective metrics: new timing deltas, parasitic extraction compare on netlists, mask level – flash counts per mask and comparing to final, process test examples, etc.
  - Important to ensure the whole system, not just the chip - methodology needs to be expandable to the overall system.
- DMAG saw need for a fourth LoA that a component / system would have absolute assurance as opposed to other three levels.
  - Important consideration for equipment in missions that cannot fail or be compromised (e.g., Nuclear Weapons and Delivery Systems).
  - LoAs map well to industry practices but need a fourth LoA pushing barrier to the absolute max would be appropriate.
  - Most critical industry applications demand and require 100% test pattern coverage, 100% fault isolation, and defect characterization.
- Executive agent required but JFAC is a very small group and not sized at this point to take on this task, JFAC would have to change to take a role of this scale.
  - Private sector participation will be required – that's where most of the experts are – organized like an "FAA committee".
  - JFAC could oversee the committee.

"Critical for DoD to pick up on these commercial best practices."

Further Observations and Feedback

Defense Innovation Unit (DIU), Space Portfolio – 31 January 2023

- DIU's mission -- accelerate adoption of commercial tech, to transform military ops while building/growing national security innovation base
- U.S. must transform space operations from expendable (self-contained) to serviceable (modular) spacecraft systems and architectures
    - Impact on ME is significant – space systems can then be repaired or replaced, reducing consequences of radiation total ionizing dose over lifetime of a modular component
- Emerging commercial space sector relies on COTS microprocessors from large scale manufacturers, which include subset that can be characterize as radiation-tolerant (e.g., Falcon 9 reusable launch vehicle, which does not use radiation-hardened ME)
- **DIU's perspective – the growing demand for proliferated space systems in LEO and shift to modular, serviceable spacecraft and architectures in MEO, GEO, and cislunar space . . . will accelerate demand for low cost, advanced microprocessors available only from large, state-of-the-art production facilities**
- DIU is experimenting and prototyping commercial solutions that employ radiation-tolerant COTS microelectronics
    - If T&AM team needs guidance on how long these systems need to be viable, DIU can give guidance
    - Most significant prototype activities include the Hybrid Space Architecture (HSA), which seeks to establish IoT architecture in space that is software-defined, scalable, and serviceable in orbits beyond LEO
- For testing, DIU can use its existing ride-share contracts to collaborate with small and large-scale chip manufacturers to test designs
- DIU currently has no access to DoD CHIPS Act funding and believes a well-balanced portfolio within OUSD (R&E) should include investigation of commercial, rad-tol microelectronics solutions

Outline of Detailed Exposition of Findings

- Technical Evaluation of Attack-Tree Countermeasure Analysis
- Assessment of Pilot Program Activities
- Stakeholder Engagement and Perspectives
  - U.S. Government Stakeholders
  - Commercial Stakeholders

Goal

Determine if strategies already adopted by commercial industry to ensure the security and integrity of their products are compatible with the proposed MQA approach

- Specifically what strategies does industry implement to achieve security, confidentiality, integrity, and availability (e.g. Supply Chain Risk Management, SCRM) in their products?
- What commercial SCRM standards exist that are industry-originated and/or widely adopted or respected by commercial suppliers?

SCRM strategies provide the basis for commercial industry to ensure the security and integrity of their products

High-Level Approach

- Conduct background research on standards for hardware assurance and security
- Participate in ANSI Section 224 Workshop
- Develop list of outside companies and organizations to engage with across the ecosystem
  - Perform initial outreach; typically informal discussions
  - Schedule more detailed interviews
  - Follow ups as necessary
  - Hoping to keep discussions open (no NDA); may limit depth of detail or source
- Collect as much input as we can with an outside perspective

Details of Commercial Findings and Observations (1/6)

- Industry asserts it follows all applicable laws and regulations in its business practices
- Industry-wide standards represent consensus of participating companies on how to deal with security SCRM issues (e.g., ISO 9001, ISO 27001/27002, ISO 20243, IETF SCITT, NIST Publications)
  - Lots of other standards may have applicability or use in microelectronics (e.g., ISO, SEMI, Accellera, IEEE, JEDEC, SAE, IPC, IETF, Trusted Computing Group, Open Group, Assura, PSA, SESIP, CSA, fido, OMG, OPC, iic, IEC)
  - Best practices
  - Standards and practices are compatible with MQA
  - Did not find a standard or set of standards that are equivalent to MQA
- Companies generally cite compliance with these standards and with best practices in their public corporate policy statements and tout partnerships and supplier relationships, continuous monitoring, audits, quality improvements programs, cyber and security groups, problem tickets and reporting
- Industry is aware of security concerns in general; growing concerns about security throughout supply chains
  - Mainly handling specifics though internal practices – e.g., NDA's, disclosure of breaches
  - Commercial industry doesn't seem very concerned with foreign partners from assurance perspective
  - Industry sets security expectations in contracts with suppliers; monitor through lifecycle

Details of Commercial Findings and Observations (2/6)

- Some outside stakeholders that said they were aware of MQA reported they thought it was still more of a development effort and not yet ready for implementation
  - Gov't response indicated a fabless co. involved in MQA had adopted some of the practice for their business
  - Sharing data can require senior-level approvals
  - Sharing 3rd party IP can be difficult due to NDA's and license/use agreements
- On Assurance from suppliers – most stakeholders indicate their long-term partnerships and trusted relationships, lack of any specific concerns on trustworthiness (some have special practices including litigation options in this area)
- On their own Assurance – most stakeholders say their service/product is their reputation and use internal practices to produce at highest quality and lowest price ("I put my name on this")
- On the need for additional assurance efforts – most stakeholders say they do not share the need for themselves for additional measures at this time but are always re-evaluating; unknown unknowns…
  - Industry has experienced losses of IP but hasn't faced existential threat in products, generally follow the innovation model to product evolution (run faster)
- Some assurance aspects may be difficult to standardize – semiconductor design/fab/packaging tech change with almost every generation
- Standards not typically cited in some areas – design, IP generation, but practices matter

Details of Commercial Findings and Observations (3/6)

- IP providers provide reference flows and various other types of IP for test and verification so chip designer can check IP performance and function
  - IP vendors concerned about export control have determined country(ies) of origin for their IP
  - Haven't been requests typically from commercial customers for disclosure of meta data on IP, focus on performance
  - High volume licensees generally have more influence over IP vendor
- IP vendors are reputation businesses and see themselves as partners with their customers
  - Widely used IP very unlikely to harbor anything malicious
- Most customers say that more complete IP information for assurance purposes is usually available but can be costly to obtain
  - Difficulties with multi-party NDA's and license/use agreements for sharing IP with third parties for verification purposes
- Emerging IP standards may serve IP providers interests to protect information, e.g., incorporation of encryption and obfuscation of IP can make independent validation and verification very difficult
- Some noted that some customers can make unusual requests or insistences in this area, and that their negotiations and/or agreements to comply almost always goes into the larger business-case decision but generally companies don't want to repeat the work done by suppliers
- Some noted that as new methods for assurance go into practice, future products should benefit

Details of Commercial Findings and Observations (4/6)

- Some large DIBs have their own Foundries
  - Have steady-state demand with Commercial customers
  - Would be challenging to keep Foundries open only with DOD buying every now and then
- Most commercial firms vet vendors before they buy from them (this is especially true if they have a national security mission, and/or are selling to DOD, or seeking to do so)
- Most/all DIBs, Space companies and Start-ups are not procuring Chips from China, and/or won't work with China
  - Some smaller firms work w/TSMC through middle-man since TSMC has high "volume-buy" requirements
  - One well-funded start-up noted that it's not concerned about TSMC stealing IP, and has more concern with Samsung who is also an integrator (i.e., makes their own products)
- Many companies follow their company's more stringent "Corporate" Policy over any policy DOD has
  - Several noted vetting is "corporate, financial, and technology"
- Many companies buy "COTs" from reliable vendors
- One firm commented that for "mission threats … there is a lot more than *chips* to consider, and maybe chips are not the weak point of entry"

Details of Commercial Findings and Observations (5/6)

- The large DIBs we spoke with are *all* selling to the DOD (and NASA), and adhere to the DOD and NASA requirements, including the need for "rad-hard, or rad-tolerant" components
  - NASA requirements are more stringent than DOD
  - NASA has ultra-low tolerance for mission failure (e.g., Artemis Program)
- Space companies noted that whether they are selling to DOD, or NASA, or commercial firms, they often have "rad-tolerant or rad-hard" requirements to meet
- For some Space companies, cybersecurity is important, even if they are not selling to DOD
- One Space firm noted that their products/services must meet GEO requirements (e.g., must be built to last 10 years+, or they lose revenue)
- On related front, one company we spoke with was foreign-owned, has CRADA w/DOD, and expects to sell to DOD
  - Made it a strong point to share that while onerous, DOD has a good "FOCI-firm" process to enable foreign companies to sell to DOD; NASA doesn't have this (e.g., which can hurt U.S. industrial base)
  - DOD's FOCI process enables DOD to benefit from foreign owned capabilities and investments made in U.S.

Details of Commercial Findings and Observations (6/6)

- Many firms noted they do stringent background checks when hiring, and/or require employees to be cleared
- One Space firm commented that its employees who have access to designs must be U.S. citizens
- For large DIBs, a consistent theme is that they “build secure products, not just security into products” and often have a lot of customer oversight in work they do for the DoD
- Many firms do extensive testing of products
- For custom components, many firms buy from Trusted vendors and put through rigorous process
- Another firm noted that “humans in supply chain must trust each other, and not just rely on supply chain mapping
  - Example was given that “SpaceX is deploying humans to make sure sensitive components in satellites are ok”

Industry Sectors with Vested Interest in Security, Confidentiality, and Integrity in Their Products

- **Automotive**
  - Long product life
  - Recall/fix is very expensive process
  - High product liability consequences
  - Brand equity
- **Aerospace**
  - Failure can have catastrophic consequences
- **Medical device manufacturers**
  - Rigorous FDA approval process
- **Healthcare**
  - Privacy of personal healthcare data
- **Communication**
  - Secure switching and interconnection
- **Critical infrastructure**
  - Potentially massive impacts of failure
- **Insurance**
  - Reduce underwriting liability

These industries have substantial financial incentive to employ SCRM to ensure the security and integrity of the microelectronic components contained in their products

Hardware Assurance Failure Levels (Industry)

- **Level A. Failure Condition Classification** – **Catastrophic**

  Hardware function whose failure or anomalous behavior would cause a failure of system function resulting in a catastrophic failure condition. Level A is most critical, with a classification for failure condition of "catastrophic," for example, "failure conditions that would prevent continued safe flight and landing." While effects on occupants are not defined for this level, fatal injury to many of the occupants would probably result.

- **Level B. Failure Condition Classification** – **Hazardous/Severe-Major**

  Hardware function whose failure or anomalous behavior would cause a failure of system function resulting in a hazardous/severe-major failure condition.

- **Level C. Failure Condition Classification** – **Major**

  Hardware function whose failure or anomalous behavior would cause a failure of system function resulting in a major failure condition.

- **Level D. Failure Condition Classification** – **Minor**

  Hardware function whose failure or anomalous behavior would cause a failure of system function resulting in a minor failure condition.

- **Level E. Failure Condition Classification** – **No effect**

  Hardware function whose failure or anomalous behavior would cause a failure of system function with no effect on operational capability

Hardware Assurance Failure Levels (DoD)

- **LoA3** - If the system fails, the consequences will be extremely grave. If the system is subverted, it can **cause exceptionally grave harm** to U.S. personnel, property, or interests. A failure or subversion of this system:

  May represent an existential risk to the USG, and
  May cascade across many DoD systems in a way that impacts total operational readiness in an immediate way, and
  Will interrupt essential operational capabilities of the DoD.

- **LoA2** - If the system fails, the consequences will be grave. If the system is subverted, it can cause **serious harm** to U.S. personnel, property, or interests. However:
  - Essential operational capabilities for the DoD may be degraded during a system failure, and
    - Redundant capabilities can be brought online as part of a continuity of operations plan, and
    - The failure of the system will not cause cascade effects across many DoD or allied systems.

- **LoA1** - If the system fails, U.S. Government (USG) capability will be **reduced in a meaningful way**. If the system is subverted, it can cause harm to U.S. personnel, property, or interests. However:
  - Essential operational capabilities for the DoD will remain available even during a system failure.

Impact of commercial hardware assurance failure parallels impact in DoD systems

SCRM: Defined in the NDAA 2020 Language Best Practices

*Further **Section 224** directs that the Secretary shall, to the greatest extent practicable, ensure that the requirements of the Department and the acquisition by the Department of microelectronics enable the success of a dual-use microelectronics industry.*

Sources Guiding Commercial Suppliers SCRM Strategies

Through in-depth interviews and monitoring industry standards bodies, NIST has developed a set of "best practices" that is widely adopted by industry and the DOD

NIST- Key Practices in Cyber Supply Chain Risk Management: Observations from Industry

1. Integrate C-SCRM Across the Organization
2. Establish a Formal C-SCRM Program
3. Know and Manage Critical Components and Suppliers
4. Understand the Organization's Supply Chain
5. Closely Collaborate with Key Suppliers
6. Include Key Suppliers in Resilience and Improvement Activities
7. Assess and Monitor Throughout the Supplier Relationship
8. Plan for the Full Life Cycle

NIST Report NISTIR 8276, published February 2021

National Counterintelligence and Security Center
Supply Chain Directorate
Published 04/05/2019

NATIONAL SUPPLY CHAIN INTEGRITY MONTH - *CALL TO ACTION*

BEST PRACTICES

Obtain Executive Level Commitment for a Supply Chain Risk Management (SCRM) Program

Build an Integrated Enterprise Team. A successful SCRM program requires commitment from senior stakeholders from across the enterprise including Security, Information Assurance, Insider Threat, Legal, and Acquisition.

Communicate across the Organization. Horizontal and vertical communication is essential to ensure senior stakeholders' investment in the success of a SCRM program. This includes information sharing to inform risk decisions and implement mitigations.

Establish Training and Awareness Programs. Organization-wide awareness and training further embeds the SCRM practices with senior stakeholders and empowers employees to manage, mitigate, and respond to supply chain risks.

Identify Critical Systems, Networks, and Information

Exercise Asset Management. Real-time knowledge of the location and operational status of all assets is essential to understanding what systems, networks, and information are critical to the enterprise.

Prioritize Critical Systems, Networks, and Information. Identifying critical systems, networks, and information enables stakeholders to prioritize resources for protecting these systems and mitigating supply chain risks.

Employ Mitigation Tools. Continuous monitoring of system data and network performance enables rapid implementation of appropriate countermeasures to minimize the impact of an attempted disruption or attack.

Manage Third Party Risk

Conduct Due Diligence. Assess first-tier suppliers regularly to increase visibility into third-party suppliers and service providers. Leverage this data to properly vet vendors who are providing key components to critical systems and networks.

Incorporate SCRM Requirements into Contracts. Use SCRM-related security requirements as a primary metric – just like cost, schedule, and performance - for measuring a suppliers' compliance with the contract. These security requirements include personnel security and system and services acquisition, and are fully described in NIST SP 800-161.

Monitor Compliance. Monitor suppliers' compliance to SCRM-related security requirements throughout the supply chain lifecycle, even when terminating supplier relationships.

NC&SC SCRM "Best Practices" map onto NIST identified commercial "Key Practices"