# Trusted Microelectronics

# Joint Working Group

## Executive Summary and Recommendations

**July 2017**

DISCLAIMER: The ideas and findings in this report should not be construed to be official positions of any of the organizations listed as contributing members of this Joint Working Group or the membership of NDIA. It is published in the interest of information exchange between Government and Industry, pursuant to the mission of NDIA.

(This Page Intentionally Blank)

# I. TABLE OF CONTENTS

(This Page Intentionally Blank)

# 1 EXECUTIVE SUMMARY

The members of NDIA are dedicated to maintaining the technical superiority of U.S. defense and national security systems. Today the ability of U.S. corporations and Government agencies to acquire advanced semiconductor devices has been severely undermined by the evolving semiconductor industry which is driven by commercial demands for consumer products, coupled with producer consolidation caused by profitability concerns.

Not only do our potential adversaries now have access to the most modern technology, in some cases they have become the major suppliers of the very technology we have come to rely on to establish our technological superiority. The question becomes: Who can we trust?

> "…with the continued diffusion of advanced technology, U.S. military technological superiority is no longer assumed and the dominance U.S. forces have long enjoyed across the land, air, sea, space, and cyberspace domains is no longer assured."
>
> - *House Report. 114-537 - National Defense Authorization Act For Fiscal Year 2017*

Virtually every system used for Defense and National Security depends on advanced semiconductor devices. Recognizing this reliance, and coupled with trends in the industry towards off-shore suppliers, NDIA organized a series of workshops on assured microelectronics supply and as a result in May 2016 launched the NDIA Trusted Microelectronics Joint Working Group (TM JWG).

**Approach**

The TM JWG self-organized into four primary teams, each addressing a critical aspect of the challenge to obtain the trusted and assured defense microelectronics required for national security:

1. ***Future Needs & System Impact of Microelectronics Technologies****, led by Charles Adams, Northrop Grumman Corporation*
2. ***Trustable Access to Leading Edge Technology****, led by Ezra Hall, GLOBALFOUNDRIES, Inc.*
3. ***Trustable Microelectronics Standard Products****, led by Kenneth Lebo, Jacobs Engineering Group Inc.*
4. ***New Methods to Instill Trust in Commercial Semiconductor Fabrication****, led by W. Pat Hays, The Boeing Company*

Over the 14-month study period, the NDIA TM JWG membership reached 80 participants from nine government offices, 28 separate defense companies, and nine non-profit and FFRDC organizations. The deep and diverse expertise of the NDIA TM JWG members was leveraged to tackle semiconductor challenges specific to defense and national security programs.

Our teams analyzed approaches to assure semiconductor availability for defense systems through strategy development, research initiatives, standards participation, demand aggregation, and future requirements integration. Their findings should add value to the Department's ongoing microelectronics strategy development by representing the defense industry's concerns and recommended solutions.

## 2 KEY RECOMMENDATIONS

These are the key recommendations resulting from the work of the four teams of the joint working group:

***Create a U.S. National Semiconductor Strategy***

The absence of a comprehensive national semiconductor strategy was viewed by the TM JWG as a major impediment to assuring access to critical national security technologies and to U.S. technological competitiveness. The TM JWG recommends creating a Government-Industry-Academia consortia or coalition to develop a national semiconductor strategic plan, including and beyond DoD's requirements, complete with stretch goals, major priorities, and desired outcomes. This plan would prioritize essential technologies for loss contingency protections and create a technology roadmap to identify investments that will strengthen the U.S. semiconductor industrial base, and that connects domestic semiconductor capabilities and projected demand.

***Adapt DoD Acquisition Practices to Align with Commercial Market***

The TM JWG's analyses highlight the differences between DoD's acquisition practices and commercial sales priorities. The TM JWG recommends defense programs be provided new methods to purchase technology on commercial terms after the commercial products have been evaluated for trustworthiness. Further work is recommended to adopt commercial solutions and intellectual property with well-defined risk mitigations and to develop a process to plan sustainment needs during initial product purchases.

***Increase DoD Market Influence***

The DoD's share of the semiconductor market has dramatically declined to less 1% share of today's semiconductors consumption and the Department's ability to gain access to needed microelectronics capabilities has correspondingly diminished. The TM JWG suggests actions that can increase market influence by exchanging research investment for access to commercial products; and, aggregating demand across DoD programs, other USG offices, and non-USG industries that have similar component and system integrity concerns.

***Adopt New Trust and Assurance Models***

The JWG's analyses articulated the value of developing program-specific Trust Plans and Technical Implementation Guides to identify security measures for each step in the product flow from design through test. The Guides would factor technology-enabled mitigations and countermeasures into security requirements; the Plans could expand today's Trust offerings by defining the boundaries for assurance spectrums or "tiers of trust" levels, and would cover component categories beyond ASICs.

***Launch R&D to Achieve Trust / Security in Un-trusted Fabs***

Separate from, but coordinated with, the national semiconductor strategic plan, the TM JWG recommends launching near-term research and development to address the security concerns of existing commercial technology capabilities, including Trusted 3D/2.5D integration, to leverage these capabilities for defense systems. Establishing a government focus to track future technology trends and impacts is recommended to continuously identify technology renewal opportunities and capabilities gaps.

# 3 JOINT WORKING GROUP TEAM SUMMARIES

The four primary teams of the TM JWG each addressed a critical aspect of the challenge to obtain the trusted and assured defense microelectronics required for national security. Each of the teams has created a white paper that details purpose, methodology and recommendations. These papers are summarized here.

## 3.1 Team 1 - Future Needs & System Impact of Microelectronics Technologies

A diverse group of semiconductor industry, defense primes, USG (primarily DoD), and non-profit research institute professionals was assembled as a part of the Joint Working Group to look into the future of microelectronics and specifically how that future will impact the economic well-being and defense of our country. The combined members of this group had specific and deep understanding of semiconductor technology, including how it is specified, designed, manufactured, deployed, and managed within both DoD systems and commercial applications. The Team addressed both the demand side and the supply side of microelectronics for the Defense industry.

The Demand Side: The Team examined the likely future needs, specifically over the next 5-10 years, of end-user systems (both DoD and commercial but focusing on the former) that utilize microelectronics. We investigated and discussed a wide of a range of defense applications and future systems to guide our thoughts about current and future demand for semiconductor and microelectronic component technologies

The Supply Side: Then we reviewed the emerging supply issues of new semiconductor technologies that will enable, impact, and potentially dominate these systems, as well as some of the concerns as to trust and assurance of this supply. The group utilized its collective deep technical knowledge in the context of the demand side and looked for categories of emerging technologies that might benefit the entire spectrum of US defense, government and US commercial interests as well. The emerging technology categories included:

- *3D / Heterogeneous Integration*
- *Compound Semiconductor*
- *Deep Node CMOS*
- *Other Novel Technologies: Advanced Digital, Analog Computing, Neuromorphic and Quantum*

As we looked at the specifics of these technologies against the backdrop of today's known issues of assured secure access (concerns about the integrity and USG availability of commercially developed semiconductor products are well-documented), we identified a number of consistent themes. Moreover, as these themes were discussed by a focused group of experts – a single unifying recommendation emerged, along with a number of important sub-recommendations.

### 3.1.1 Summary of Findings and Recommendations

This team examined the four primary new and emerging technology categories listed above and discussed what concerns and challenges came to mind and what new mitigations to those challenges might be put in place. The team concluded that:

- *The agility and pace of USG efforts in future microelectronics technologies will be unlikely to match the accelerating pace of Industry. Methods for addressing this "cultural mismatch" must be developed.*
- *The proliferation of readily available commercial technology and the sophistication of adversaries will not decrease, it will dramatically increase. Threat vectors will numerically increase and attack surfaces will also multiply. Advanced commercial technologies will be available to all (including adversaries) so we must develop secure methods to extend/augment COTS' capabilities to ensure the DoD has differentiating capabilities to maintain superiority.*
- *A wide range of new technologies will be coming out of a broad set of international commercial players. Diversity of technology and sources of that technology will increase as scaling based progress is replaced by other innovative approaches (new designs, heterogeneous integration, architectures and devices). The DoD has a unique opportunity to influence the direction of key emerging technologies thereby helping assure a US Industrial base which provides future DoD access and benefits the US economy as a whole.*

**Key Team recommendation**: Create a U.S. National Semiconductor Strategy
While the US military global superiority and independence depends on eternal vigilance, our strength originates from constant technological innovation.

## 3.2 Team 2 - Trustable Access to Leading Edge Technology

This team examined the challenges of maintaining access to trusted sources of State-of-the-Art (SOTA) microelectronics and addressed the potential consequences of continued off-shoring of state-of-the-art microelectronics manufacturing, China's anticipated investments, and the economic and national security implications of these developments. The team also addressed possible mitigating actions to sustain the U.S. defense microelectronics industrial base.

The team concluded that there is a serious risk that the USG could completely lose access to trusted sources for SOTA microelectronics, due to the mismatch between commercial business models of the semiconductor industry (particularly SOTA manufacturers) and the USG acquisition process. Without strategic and affirmative action, it is likely that off-shoring of microelectronics manufacturing will continue, increasing this risk to the USG. The USG purchasing power is insufficient to influence today's commercial industry, so access depends both on the presence of domestic SOTA manufacturing and how well USG acquisition is aligned with market practices for access to that base. Without trusted sources for the USG's critical microelectronics needs, dedicated adversaries could steal vital information or manipulate military systems.

### 3.2.1 Summary of Findings and Recommendations

The team examined several actions that could be taken to counteract the effects of continued off-shoring, ranging from economic, to technical, to educational. The major conclusions detailed in this paper include:

- *Accessing commercially available design intellectual property (IP) and microelectronics design capabilities is key. Creating a database or repository of "Trusted IP" and/or a leading-edge chip design capabilities through a public/private partnerships or consortium would help maintain and assure future design and IP access.*
- *Aggregating demand for trusted, secure microelectronics across government –beyond the national security mission agencies– would increase the government's negotiating power with commercial manufacturers and could possibly streamline the acquisition process for technologies.*
- *Increasing the universe of communities that value hardware security, within the private as well as the public sector would greatly increase the demand for more robust security and authentication measures for SOTA microelectronics. This larger community of*

*interest comprises the utilities and transportation sectors, and numerous commercial industries, including avionics, automotive, Information Technology (IT), medical devices, finance and others.*

- *Expanding the USG's framework of microelectronics Trust (as defined in DoDI 5200.44) to multiple levels of trustworthiness incorporating countermeasures, and expanding it to include assurance for catalog items (Field Programmable Gate Arrays (FPGAs), Commercial Off The Shelf (COTS), Government Off The Shelf (GOTS), Military Off The Shelf (MOTS), etc.), would give defense programs more options for building trusted, secure systems. Such an expanded framework should allow programs to better leverage existing hardware security measures for a wider range of microelectronics and thus increase the overall security of the entire system while simultaneously enabling greater access to SOTA at a lower overall cost to the USG.*
- *Creating public-private R&D partnerships would improve the USG interface with the semiconductor industry in many ways. Public-private R&D partnerships could foster a robust domestic supply chain for future technologies with earlier USG access. They could also provide the USG with a vehicle to test out new contract mechanisms on small scales, potentially improving the overall acquisition process. Additionally, it would provide a pipeline for training USG engineers in leading edge technologies.*

No single action is a silver bullet for the USG's access problem. Therefore, a comprehensive and coordinated approach is necessary to ensure the availability of trustworthy microelectronics. The primary recommendation of this team is to develop a coordinated, national strategy for ensuring government access to trusted SOTA microelectronics, combining current trust approaches with recommended USG process reforms and broader economic support of the domestic semiconductor industry. Such a national strategy should aim to align government practices with those of the commercial industry, strengthening the industrial base, preserving USG access to the leading edge, and improving hardware and software security more broadly in critical industrial sectors.

## 3.3 Team 3 - Trustable Microelectronics Standard Products

Catalog microelectronics components and technologies designed and produced for commercial markets are often used in defense systems and can be critical to the system's function and operation. While the Department of Defense (DoD) has established trust criteria for sourcing custom integrated circuits used in covered systems, there is not an equivalent trust criteria covering commercial standard parts. Team 3 of looked at this question by analyzing adjacent non-defense industries and the lifecycle of standard products. Several adjacent industries have concerns similar to DoD's and thus present an opportunity to join their initiatives to create new standards and controls.

While commercial catalog components come without any evidence of meeting any defense specific trust or assurance requirements, visibility into commercial practices can provide for some level of characterization of trust and assurance. It should be noted that Defense Microelectronics Activity (DMEA) recently created a process to allow commercial parts to achieve a Category II level of Trust. This new criterion requires participation by the vendor and as such is not addressed in this paper.

### 3.3.1 Summary of Findings and Recommendations

There are tremendous upsides with using commercial microelectronics. For example, defense systems can be afforded highly advanced components such as FPGAs, memory chips or receiver chips that might have cost over $100 million to develop and bring to market, but sell for a small fraction of the development cost from amortizing that cost across the commercial applications' volume manufacturing. Catalog chips that are in wide use would conceivably be subject to global security challenges and evaluations with corporate documentation of errata or issues of fixes addressed via firmware updates etc., thus improving the component's reliability over time.

On the downside, using commercial components coupled with long-lived defense systems can create long-term obsolescence problems for Defense systems as the life-cycle of chip technologies becomes shorter and shorter. From a security perspective, a commercial component might be susceptible to an unpublicized vulnerability for an adversary to exploit if enough effort were spent examining the chip. Of course, it is possible for a custom or semi-custom chip to have an analogous flaw, but if it were produced using a trusted flow it is presumed to be difficult for an adversary to obtain the chip and the design information needed to exploit the flaw.

The NDIA Trusted Microelectronics Joint Working Group Team 3 recommends that DoD:

- *Develop and employ a consensus approach for establishing categories of trustworthiness for catalog chips based on risks, commercial practices, use of standards (SAE, ISO or Open Group accreditation procedures etc.) or quantifiable supplementary information that can be supplied with respect to a catalog chip. This approach should lead directly to a methodology for assessing individual microelectronics used in critical roles in defense systems. Using a categorization approach to establish various levels and mitigations will require expert inputs and debates but will provide the best long-term solution for DoD.*
- *Partner with non-defense industries working with commercial microelectronics companies to enhance security status and affordability of catalog chips in areas like industrial standards and supply chain practice.*
- *With vendor participation, the DMEA Category II criteria could be used for an additional level of trust above the basic best commercial practice.*

## 3.4 Team 4 - New Methods to Instill Trust in Commercial Semiconductor Fabrication

Team 4 evaluated new technical methods to instill trust in semiconductor fabrication with the goal of determining if these methods can instill sufficient trust in commercial fabrication to meet the requirements of sensitive DoD programs. Unlike prior surveys, Team 4 evaluated which methods which can be readily and pragmatically applied. For this purpose, trust is defined as "the confidence in one's ability to secure national security systems by assessing the integrity of the people and processes used to design, generate, manufacture, and distribute national security critical components."

This report recommends development of a new review process to enable approval of trusted access to commercial fabrication for selected military end use semiconductors. The Defense Microelectronics Activity (DMEA), under the Office of the Secretary of Defense, is the program manager for the Trusted Foundry Program and, as such, is the clear candidate to implement this report's recommendations.

DoD semiconductors require trust throughout the development process starting with electronic design automation (EDA) tools and 3rd party intellectual property; however, Team 4 focused on trust in the fabrication phase because traditional means, using DMEA-accredited Trusted Foundries to achieve trust in semiconductor fabrication, are not available at advanced process nodes, potentially precipitating a crisis for DoD. Unmitigated, this crisis could disadvantage DoD with asymmetric semiconductor capabilities and/or undermine DoDI 5200.44 with increasingly frequent waivers of its Trusted Foundry requirements.

### 3.4.1 Summary of Findings and Recommendations

Although the primary goal of Team 4 has been to open trusted access to commercial semiconductor fabrication, it is important to note that the same methods can be applied to increase the security of semiconductor fabrication within the current Trusted Foundry program, while extending the program's offerings.

The new methods discussed in the team's paper have the potential to instill Confidentiality and Integrity in semiconductor fabs which are outside the DMEA Trusted Foundry program. Whether the risks can be sufficiently mitigated to enable commercial fabrication will depend on the specific IC design as well as the developer's skill in applying the appropriate methods. As Team 4 concluded, one size does not fit all. Nevertheless, under DoDI 5200.44 today, only one option is available: "In applicable systems, integrated circuit-related products… shall be procured from a trusted supplier…". To exploit the new methods as reviewed by Team 4 it is recommended that:

- *Three (3) Trust Levels be defined. The Trust Level definitions should be independent of specific implementation and instead derived from a two-dimensional "risk cube", depending on Criticality of Compromise (CoC) and the end use Threat environment;*
- *The USG program responsible for the "specific DoD military end use" should determine the required Trust Level for the ASIC;*
- *A "Technical Implementation Guide (TIG) for Trusted ASICs" be developed and maintained. This document should outline practical requirements for achieving each Trust Level, incorporating the new methods examined by Team 4 as appropriate, as well as providing developer examples;*
- *The contractor for each military end use ASIC be required to submit a Trust Plan for review and approval at PDR.*

# 4 CONCLUSIONS

Obtaining trusted and trustable leading-edge microelectronics is critical to maintaining the U.S. military's technological advantage. As foreign sources of integrated circuit design and manufacturing capabilities increase their presence in the defense supply chain, the defense industry faces increasing challenges to obtain critical electronic components both in acquisition and sustainment phases.

This is a challenge that needs to be met head-on and will not go away. The funding necessary to develop a parallel, Defense-centric, and completely isolated source of electronics for military applications is unimaginable and simply not available. The Defense establishment must adopt practices that allow it to assure itself of trusted sources of supply in what amounts to a foreign-dominated and contested environment.

NDIA Trusted Microelectronics Joint Working Group (TM JWG) was formed to collaboratively examine issues and explore potential solutions for the reduced access to assured microelectronics for defense and national security systems. With members of government, industry, non-profits, and Federally Funded Research and Development Centers (FFRDCs), the TM JWG brought diverse backgrounds to explore solutions for this common concern.

Over the course of 14 months, the four teams worked via conference calls, and occasional in-person meetings. Preliminary findings were reported at the February 2017 NDIA Trusted Microelectronics Workshop; final reports were presented at the Trusted Supplier Industry Day at GOMACTech 2017 in March.

The four teams of the Trusted Microelectronics Joint Working Group independently developed their recommendations to improve the Department of Defense's access to leading-edge, state-of-the-

practice, and legacy microelectronics critical to defense systems. The findings and recommendations from the teams have been integrated and grouped into action categories and presented here as Key Recommendations. Each team produced a more detailed white paper as their final product reflecting their conclusions.

The NDIA Trusted Microelectronics Joint Working Group demonstrates the value of government-industry collaboration when addressing critical issues facing the Department of Defense and the Defense Industrial Base. As a result of the obvious value and critical importance of this work to the Defense Industrial Base and DoD, NDIA plans to convert the Joint Working Group into a standing NDIA Division so that it may continue under an officially recognized charter.

--END--

## APPENDIX A - Terms and Abbreviations

| | |
|---|---|
| ASICs | Application Specific Integrated Circuits |
| CMOS | Complementary metal–oxide–semiconductor |
| CoC | Criticality of Compromise |
| COTS | Commercial Off the Shelf |
| DMEA | Defense Microelectronics Activity |
| DoD | Department of Defense |
| DoDI | Department of Defense Instruction |
| EDA | Electronic Design Automation |
| Fab | Fabricator of semiconductors |
| FFRDC | Federally Funded Research and Development Center |
| FPGA | Field Programmable Gate Array |
| GOTS | Government Off the Shelf |
| IC | Integrated Circuit |
| IP | Intellectual Property |
| ISO | International Standards Organization |
| IT | Information Technology |
| MOTS | Military Off the Shelf |
| NDIA | National Defense Industrial Association |
| PDR | Preliminary Design Review |
| R&D | Research and Development |
| SAE | Society of Automotive Engineers |
| SOTA | State of the Art |
| TIG | Trusted Implementation Guide |
| TM JWG | Trusted Microelectronics Working Group |
| USG | United States Government |