Trusted Microelectronics

Joint Working Group

Team 1 White Paper:

Future Needs & System Impact of Microelectronics Technologies

July 2017

(This Page Intentionally Blank)

I. FOREWORD

Over the course of the past 70 years, the United States Government (USG) microelectronics needs for national security applications [Department of Defense (DoD), Department of Energy National Nuclear Security Administration (DOE-NNSA), and the Intelligence Community (IC)] and the semiconductor industry have been intertwined. Indeed, the U.S. semiconductor industry in part grew out of USG funded Research and Development (R&D). In recent decades, however, commercial applications and high-volume production have dwarfed USG demand, such that USG purchases (be it direct or through a third party) now account for a very small part of total production, resulting in commercial market forces driving the industry. As noted by the most recent President's Council of Advisors on Science and Technology (PCAST) report,

> "The global semiconductor market has never been a completely free market: it is founded on science that historically has been driven, in substantial part, by government and academia; segments of it are restricted in various ways as a result of national-security and defense imperatives; and it is frequently the focus of national industrial policies. Market forces play a central and critical role. But any presumption by U.S. policymakers that existing market forces alone will yield optimal outcomes – particularly when faced with substantial industrial policies from other countries – is unwarranted."[1]

With global sales on the order of $335 Billion USD and worldwide R&D investment exceeding $56 Billion USD in 2015, the semiconductor industry is large and globally integrated.[2] The US currently captures about 50% of the worldwide semiconductor market with electronics being our #3 export. These trends are shown in Figure 1. The semiconductor industry is therefore very important for both the DoD (National Security) and the US economy in general.

Warfare has changed dramatically in recent years as has the enabling microelectronics requirements and capabilities. Historically, commercial digital silicon semiconductor efforts have been focused on increasing transistor density and lowering cost. The DoD requires state of the art digital component access for its advanced computation needs. Commercial RF electronics has been driven mainly by wireless and smart phone needs at fairly low frequencies and limited bandwidths.

A diverse group of semiconductor industry, defense primes, USG (primarily DoD), and non-profit research institute professionals was assembled in coordination with the NDIA as a 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.

---

[1] https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_ensuring_long-term_us_leadership_in_semiconductors.pdf, "PCAST Ensuring Long-Term U.S. Leadership in Semiconductors"

[2] Semiconductor Industry Association (SIA) – Beyond Borders Report, May 2016.

We have long prospered by allowing commercial entities the freedom to create and capitalize their products across all borders but with today's globalized world that freedom now jeopardizes our future if the Government does not plan an assured access strategy for the key microelectronic components it needs. Assured and secure access to emerging microelectronics technologies is a matter of national importance for the DoD as well as the US economy in general. The recent sales of the IBM Trusted Foundry to foreign-owned GLOBALFOUNDRIES, along with other examples of the globalization of the semiconductor market, have driven home the point that we cannot afford to lose access to critical microelectronics component sources.

This team is advocating and recommending that a National Microelectronics Strategy be created that includes a 10 year plan and supporting budget for achieving assured access to advanced microelectronics technologies.

II. PAPER DISPOSITION

This paper is formally submitted to the Assistant Secretary of Defense for Research and Engineering, Office of the Undersecretary of Defense for Acquisition, Technology and Logistics. Permission is granted to widely distribute and quote with proper attribution. The paper will be made available on the National Defense Industrial Association website (http://www.ndia.org/divisions/working-groups/tmejwg as a reference resource.

The paper includes observations and recommendations that will address the larger US Government coordinated microelectronics needs. To make progress on this critical challenge, a coordinated "whole of USG solution" (National Strategy) is required including coordination with commercial semiconductor companies and defense contractors as well as the key USG equities in microelectronics.

III. PRINCIPAL CONTRIBUTORS

Team 1 members are listed by name and company in Table 1 below. The Team met weekly via phone as well as in person on a number of occasions across approximately one year to accomplish this analysis and paper. Contributions came from virtually all members as the information, opinions, and expertise was compiled and presented in various forms to a number of audiences. The NDIA Team included industry and government experts tasked to come up with a set of recommended solutions to the future needs and systems impact of microelectronics.

Team 1 Industry and Government Contributors

	Name	Organization
1	Antonio de la Serna	DRAPER
2	Charles Adams	Northrop Grumman
3	Craig Herndon	NSWC Crane
4	Dan Radack	IDA
5	Dean Brenner	Honeywell
6	Eric Dauler	MIT Lincoln Laboratory
7	Grant Meyer	SRI International
8	Jeremy Muldavin	DASD(SE) Microelectronics Assurance
9	Jim Gobes	Intrinsix
10	Kenneth H. Heffner	Honeywell
11	Kirk Reynolds	Rockwell Collins
12	Major Manny Trejo	DoD
13	Michael Fritze	Potomac Institute for Policy Studies
14	Ray Shanahan	ODASD(SE) Anti-Tamper & Hardware Assurance
15	Scott Anderson	Lockheed Martin
16	Tim Lee	Boeing
17	Tyler Schmidt	Intel

(This Page Intentionally Blank)

IV. TABLE OF CONTENTS

V. LIST OF FIGURES

1 EXECUTIVE SUMMARY

A diverse group of semiconductor industry, defense primes, USG (primarily DoD), and non-profit research institute professionals was assembled in coordination with the NDIA as a 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 have 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 Demand Side: This Joint Working Group (JWG) examined the likely future, 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:

Formation of a National Microelectronics Strategy is Critical

Note: the scope of this paper does not include the specific tactics and policies that will be necessary to successfully create this National Microelectronics Strategy, it simply highlights why it is necessary now.

There is already grave concern today about the growing gap between commercial suppliers (many critical suppliers are offshore or owned by foreign entities) and defense needs. In the past, semiconductors and even software were created from a small number of large onshore vertically-integrated companies that had close ties and large business interests with the defense industries. The disaggregation of this industry into hundreds of international suppliers combined with commercial uses/volumes of microelectronics that far outstrip the DoD needs has created this alarming gap. This gap continues to grow.

Our examination of the sources, likely uses, and potential problems with emerging microelectronics components confirms our strong view that a National Microelectronics Strategy is imperative. This must be a National Strategy versus a Defense only strategy; this is a National Defense, Economic, Energy, and Intelligence need. Planning 10 years out is critical: beyond current short term political focus and at early development stages where USG efforts can have the most impact. It is at the early stage *formation* of new technology that US interests and secure access strategies can be best ensured. A National Strategy will need to encompass the entire lifecycle of DoD system needs (up to 50 year lifetimes and small volumes) and mesh that with the relative "mayflies" of the commercial world (< 2 years lifetimes and billions of devices). A National Strategy will also need to coordinate all key stakeholders within the US Government, the entire range of the industry from start-up to large multi-national companies, as well as the important role of universities with international students.

The existence of China's National Semiconductor Strategy cannot go unmentioned. They aim for total self-sufficiency and are investing heavily in their infrastructure. The US should not blindly emulate this approach but needs to develop its own unique strategy for ensuring long term access to secure components as well as enabling US economic vitality in this area. Creation of a practical US National Microelectronics Strategy will be a challenging multi-year process, requiring good insights into the future of the industry as well as intimate knowledge of the workings of the USG.

The authors of this paper believe that this process should start now.

2 BACKGROUND and INTRODUCTION

2.1 Background of Team 1

A Joint Working Group on Trusted Microelectronics was formed from interested parties that attended or were connected to the February 2016 NDIA Trusted Microelectronics Workshop. This JWG was then divided by self-preference into four teams. Team 1 was specifically charged with examining Future Needs & System Impact of Microelectronic Technologies from within the context of Trusted Microelectronics. Attendees of these workshops have an active interest in policies and approaches for obtaining trust in electronics (at the hardware level) and they often come from and represent a wide range of USG, FFRDCs, and the semiconductor and defense industries. They tend

to be extraordinarily technical and business-savvy in their knowledge of how things get done in the development of electronics-based systems.

David Pentrack, of the Defense Microelectronics Activity (DMEA), Dan Radack of the Institute for Defense Analyses and Catherine Ortiz of Defined Business Solutions developed an initial set of questions that could be addressed by the TM JWG. Interested participants self-organized into four teams based on their interest and expertise. The TM JWG was given the charter not only to address the pre-defined questions related to future needs and system impact of microelectronics technologies but also to explore the space for interesting areas to consider and to make recommendations as appropriate. The only caveat was the request that we work towards non-overlap with other Teams' efforts. (Teams 2, 3, 4 had similar charters: Concerns related to China and electronics, getting Trustworthiness from un-trusted parts/suppliers, and design/fab options for obtaining trusted systems, respectively.)

Our team's seed questions were:

- *What are the future microelectronics capabilities needed by defense contractors to maintain our technical advantage?*
- *Are there new hardware paradigms on the horizon that could be disruptive?*

From these seed questions, our group decided to proceed by answering the following questions starting from end-user (system) needs and proceeding to enabling components (semiconductor or more broadly termed "microelectronic" technologies) that are emerging with their adoption risks:

- **SYSTEMS:** System Needs and System Capabilities: What are the future requirements for DoD Systems?
- **ENABLING COMPONENTS:** What are the emerging technologies enabling these capabilities at the component level?
- **ADOPTION:** What are the risks regarding secure component availability (5-10 years) that enables system capabilities?

Prior to looking at the future, an understanding of today's gaps (the challenges, economics, and environment related to DoD use of microelectronics) will help the reader understand the present landscape from which we look into that future.

2.2 Today's Challenges

The following list consists of summarized categories of recognized challenges that the DoD faces today in maintaining technology superiority in today's dynamic technical world:

– Access risks of emerging technology: *Can desired technology solutions be obtained from viable sources at reasonable prices? Is assured access possible?*

- Compromise risks of emerging technology: *Can the DoD be sure that novel technology does not contain compromises to its missions?*
- *COTS risks:* *Since everyone in the world has access to the same State of the Art COTS, how can we ensure that the US capabilities remain dominant?*
- Gaps / Shortfalls: *Will the State of the Art commercial products, since they are designed with commercial intention, be good enough for the DoD missions needed?*
- Increasing Supply Chain Complexity: *Commercially available capability (Complex global infrastructure involved in SOTA designs; Fabs, IP, Packaging, Testing, etc.) is rapidly increasing accomplished through a complex disaggregated supply chain that is fragile and subject to compromise. How can it be safely utilized?*

2.3 Economic Realities

With global sales on the order of $335 Billion USD and worldwide R&D investment exceeding $56 Billion USD in 2015, the semiconductor industry is large and globally integrated.[3] The US currently captures about 50% of the worldwide semiconductor market with electronics being our #3 export. These trends are shown in Figure 1. The semiconductor industry is therefore very important for both the DoD (National Security) and the US Economy in general.

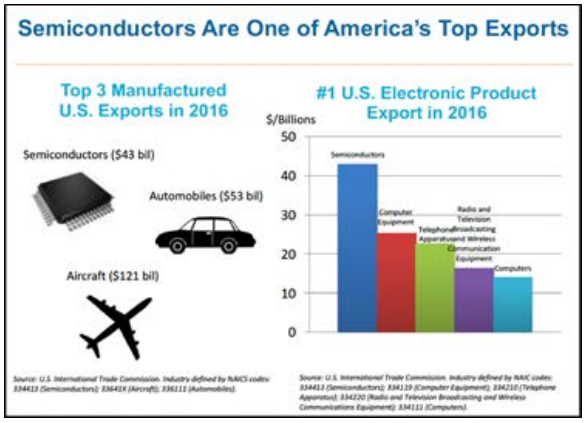

Figure 1 - The US economy has a large dependence on microelectronics. The health of the US semiconductor market is important both for DoD products and for the US economy.

There are challenges faced by the DoD including the fact that Military sales (worldwide) are now less than 1% of global sales. Figure 2 shows that since 1994 the average annual growth rate of global sales is 11.5%. This is a critical factor moving forward into the future – primarily because the money that moves (and therefore controls) these markets is no longer, for the most part, coming from USG or DoD. These drivers are now all commercial products. There has also been a migration of key supply chain elements particularly fabrication and packaging to overseas locations.

[3] Semiconductor Industry Association (SIA) – Beyond Borders Report, May 2016.

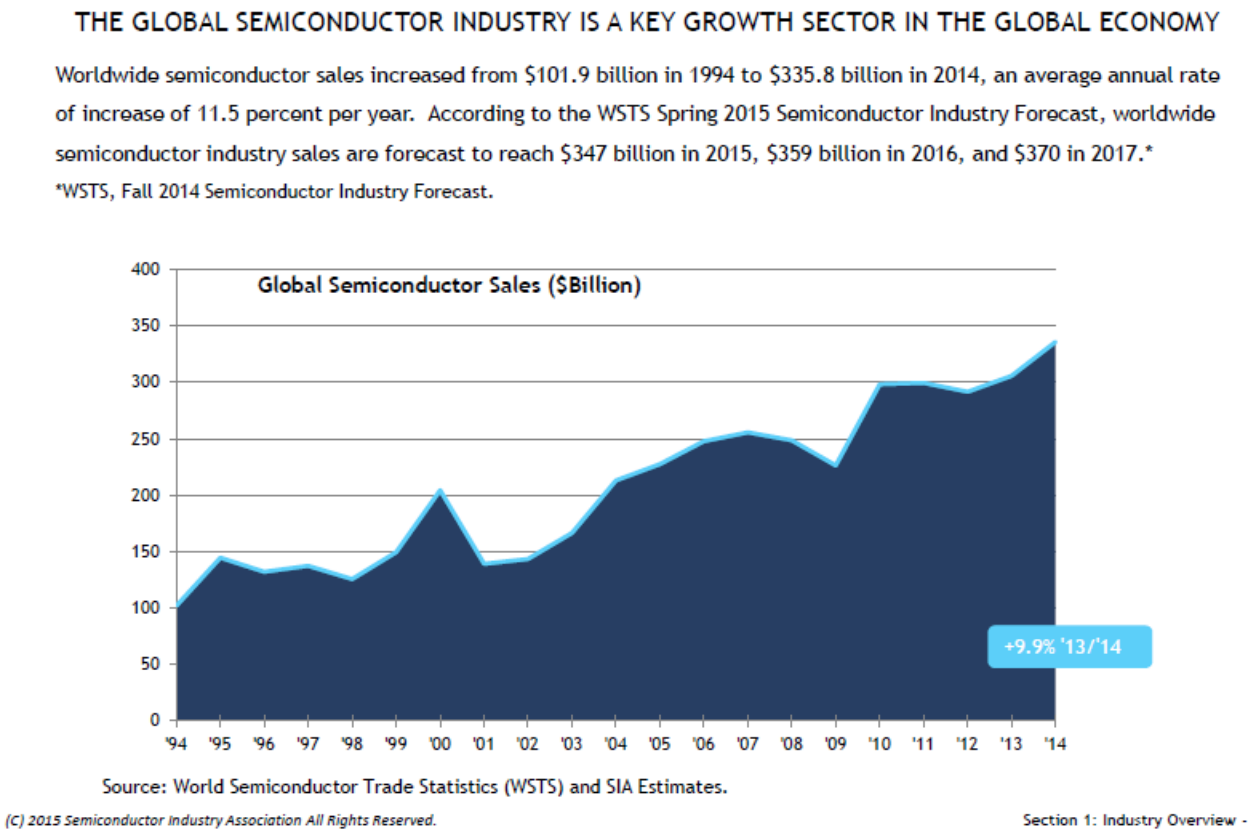

Figure 2 - Global Semiconductor Sales are a huge portion of the overall global economy. DoD has less than 1% of this business, so influence has quickly diminished over time.

3 FUTURE OF DOD SYSTEMS WITHIN A MICROELECTRONICS CONTEXT

Warfare has changed dramatically in recent years as has the enabling microelectronics requirements and capabilities. Historically, commercial digital silicon semiconductor efforts have been focused on increasing transistor density and lowering cost. The DoD requires state of the art digital component access for its advanced computation needs. Commercial RF electronics has been driven mainly by wireless and smart phone needs at fairly low frequencies and limited bandwidths. Recently, some of these commercial needs appear to be changing with higher frequency systems (5G cellular architectures) which potentially will reach into the Ka-band for large bandwidth performance. Although some DoD capabilities such as communications, radars, and sensing have similar requirements to commercial products, many require more power over wider bandwidth as well as

some unique frequencies and security requirements that the commercial side does not require. Figure 3 highlights the direction of the next generation of warfare and enabling systems. Every part of the architectures shown in this figure requires microelectronics to function appropriately.

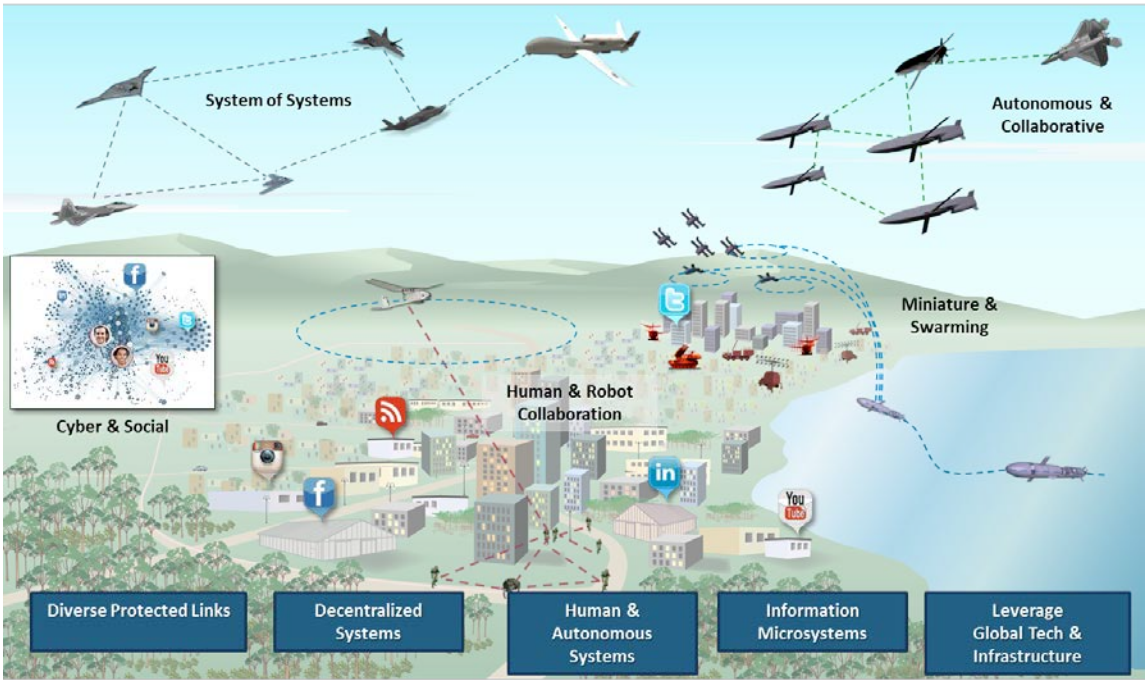

Figure 3 -Modern warfare is changing from large systems to a combination of asymmetric capabilities, multi node processing, and disparate sensing.

Some of these systems will be able to fully leverage the available commercial base of microelectronics assuming assured access to such components. Other parts of the systems, such as datalinks, space components, and imaging systems require specific DoD requirements that necessitate trust and/or very specific non-commercially available microelectronics. These include:

- Specific performance capabilities that are not required by the commercial companies
- Trust requirements that differ from commercial requirements
- Specific components that don't have a large commercial need because of the performance/price concern (specialized RF components (i.e. InP and other III-V), specialized imagers, rad-hard parts, etc.)

As a result, one addition to all of the earlier-listed challenges for DoD use of microelectronics is a the important difference between the lifespan and complexity of systems within the commercial business base as opposed to that of the Military and Intelligence Community. While modern commercial components are very complex (see Figure 4, following page), the approach to these

systems is very different than that of the military. The product lifecycle for a modern phone, for example, is around 2-3 years. Indeed, very few first generation iPhones are in use today (introduced in 2007) while fighter jets need to be serviceable for many decades.

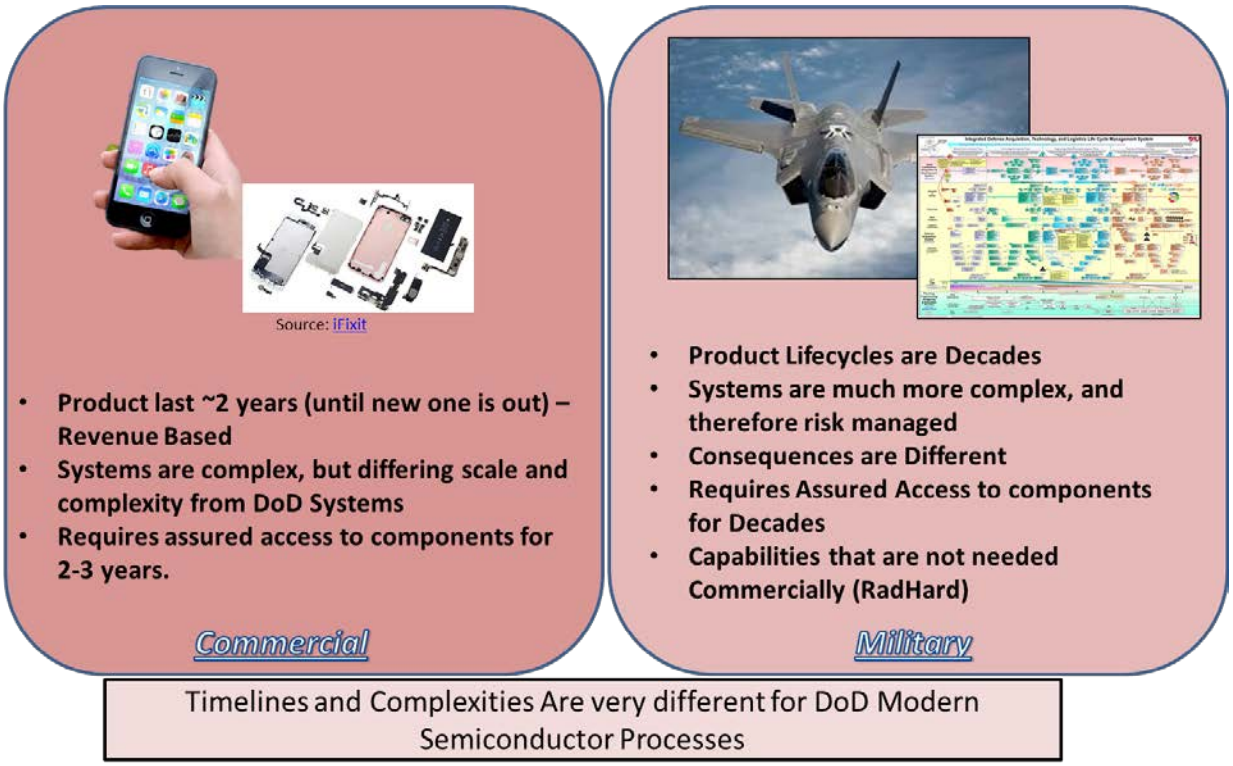

Figure 4 - Differences between commercial Products and DoD Business Models

Access must also be reiterated here as a critical challenge and concern. While access to *trusted* components is already understood as a core concern, simple *access* to the parts needed from the larger global electronics industry base is an even larger concern. Figure 5 following page) describes this concern, and emphasizes the need to take seriously the larger strategic issue of continued assured access to components for our current and future DoD systems.

This is a major concern as the globalization and consolidation of microelectronics companies is driven by demand in the commercial markets rather than by the needs within the Defense markets. Achieving continued assured access to advanced microelectronics components is imperative for the DoD to maintain the strongest Defense and Intelligence communities in the world. Without a coherent national strategy, the US government risks losing its ability to protect its key systems and the US microelectronics industry will lose its leadership role in this critical market.

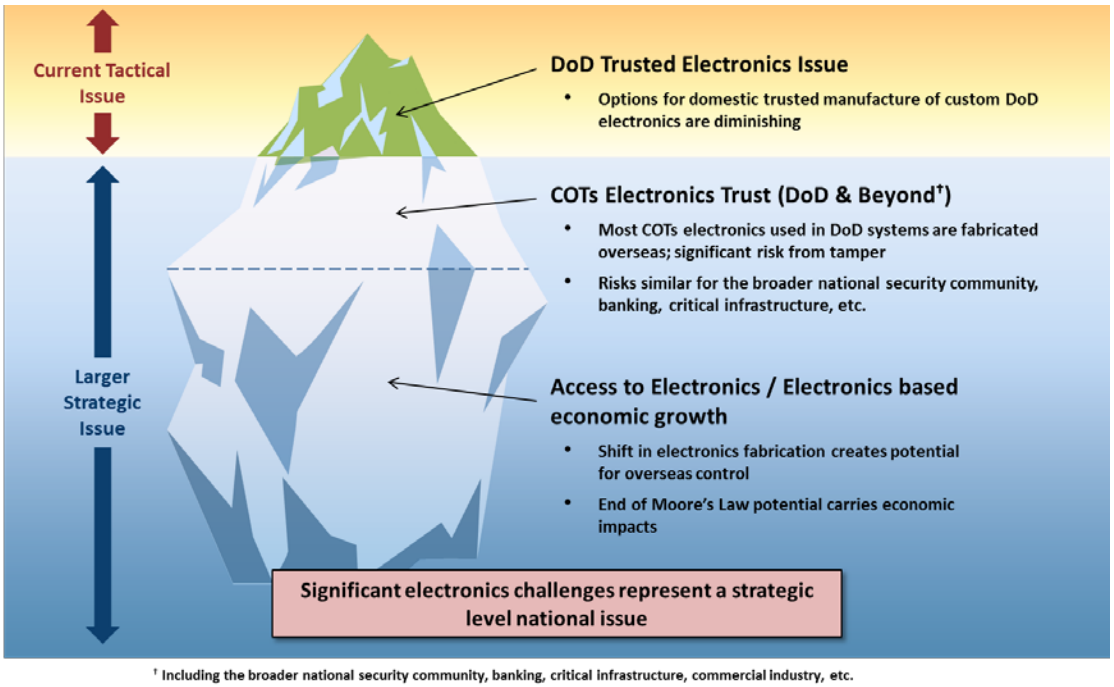

Figure 5 - Access is a critical challenge: This figure illustrates the tactical and strategic nature of the access issue.

4 DoD UNIQUE MICROELECTRONIC NEEDS

The Joint Working Group recognized, in their discussion and analysis of future systems, that today's USG and DoD systems include many cases where these organizations have unique needs for microelectronics that are not addressed commercially. A few examples identified include:

(1) Radiation hardened microelectronics for satellites and space operations.

(2) High performance Analog-to-Digital Converters (ADCs), Digital-to-Analog Converters (DACs) for Signal Processing for Multifunction RF Systems.

(3) Processors and specialized RF electronics that support the high data rate needs of EW, SIGINT, and radar systems.

(4) Compound semiconductors for high performance RF systems.

(5) Advanced Imagers.

(6) Optoelectronic components for secure communications.

(7) Anti-tamper.

The above list includes examples of microelectronic uses that MUST be manufactured solely for the DoD or USG. The list is likely to expand in the future. As can be seen in the examples of the previous section on systems and in the following section on specific future microelectronics technologies, some key USG needs require full custom capabilities and some the ability to securely customize COTS parts as well. An important conclusion drawn from this list is that it will grow dramatically: many more unique (or unique versions) of microelectronics will be needed in the future. This adds significantly to the urgency of all of the recommendations in the summary section of this pape

5 ANALYSIS OF FUTURES: EMERGING TECHNOLOGIES

Our JWG Team considered and discussed four Future Enabling Technology Categories, and our team has recommendations/considerations for each of these technologies as they apply to Future Systems. These discussions lead to our over-arching recommendations found at the end of this paper. The categories are:

1. **3D / Heterogeneous Integration**
2. **Compound Semiconductor**
3. **Deep Node CMOS**
4. **Other Novel Technologies:** Advanced Digital, Analog Computing, Neuromorphic and Quantum

The International Technology Roadmap for Semiconductors (ITRS) has been charting the progress of the semiconductor industry's march and to forecast emerging technologies that will enable the future microelectronics ecosystem. With the looming end of traditional CMOS feature size scaling, the ITRS 2.0 was recently formed focusing on "top down" drivers in contrast to the traditional "bottom up" components focus. ITRS 2.0 includes System Drivers, Heterogeneous Integration and Components, Process Integration, Devices and Structures, Outside System Connectivity, More Moore Beyond CMOS and Factory Integration. The four Categories of Enabling Technology Families we elected to investigate build on top of the ITRS commercial roadmap and address DoD-specific needs and challenges that require attention and strategies. Figure 6 shows the mapping of the four identified emerging technologies to the ITRS 2.0 Technology Roadmap. [4] Heterogeneous Integration (1) will enable the realization of microelectronic microsystems that overcome limitations being experienced due to the End of Moore's Law. [5]

[4] ITRS Semiconductor Technology Roadmap, online at http://www.itrs2.net/uploads/4/9/7/7/49775221/irc-itrs-mtm-v2_3.pdf

[5] Moore's Law, Wikipedia, online at https://en.wikipedia.org/wiki/Moore%27s_law

The semiconductor industry has successfully followed Moore's Law for nearly 50 years through continuous improvements in lithography and device scaling to achieve the doubling of transistors per integrated circuit every 12-18 months. CMOS scaling has slowed down as we approach 10 nm dimensions since critical layers now require costly multiple patterning to achieve ultra-small linewidths.

5.1 3D/Heterogeneous Integration

With each new CMOS generation, the transistors are getting faster but the signal delay (latency) due to interconnects is now dominant. Heterogeneous Integration in the form of 2.5D integration and 3D integration will dramatically reduce the interconnect distances by at least a factor of 10X for 2.5D and perhaps as high as 100X for 3D integration. Figure 6 shows how the ITRS defines two microelectronics trends: System-in-Package (SiP), and System in a Chip (SoC). 2.5D Heterogeneous Integration is a special kind of SiP technology which assembles a number of micro-bumped flip-chip mounted dies onto an interposer substrate.

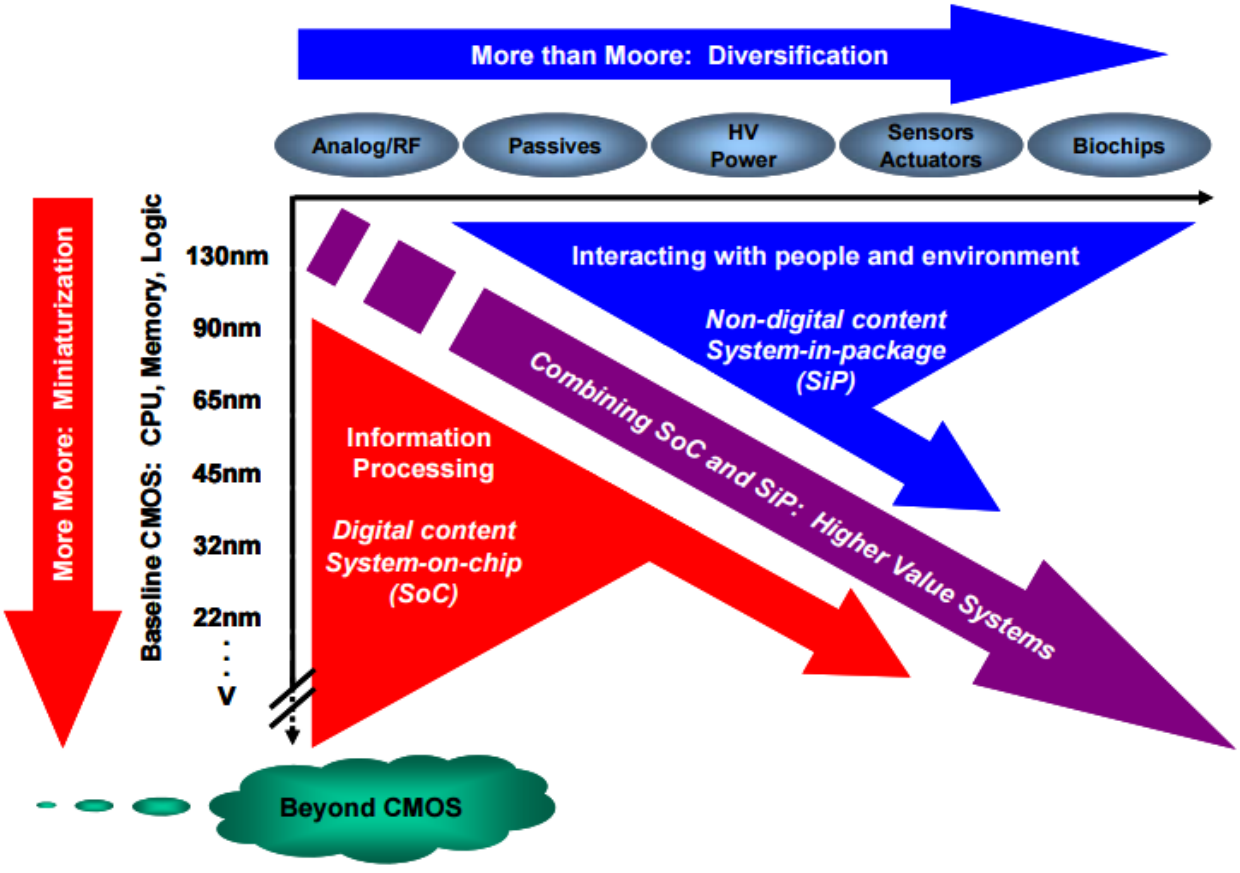

Figure 6 - ITRS 2.0 Technology Roadmap: Heterogeneous Integration Combines SoC and SiP approaches to provide an optimum solution to overcome the end of Moore's Law.

3D die stacking is rapidly maturing for 3D stacked memory for use in high performance video cards and data center servers. Figure 7 shows the many forms of SiP technologies; ranging from more conventional wire-bond attachments to die stacking.

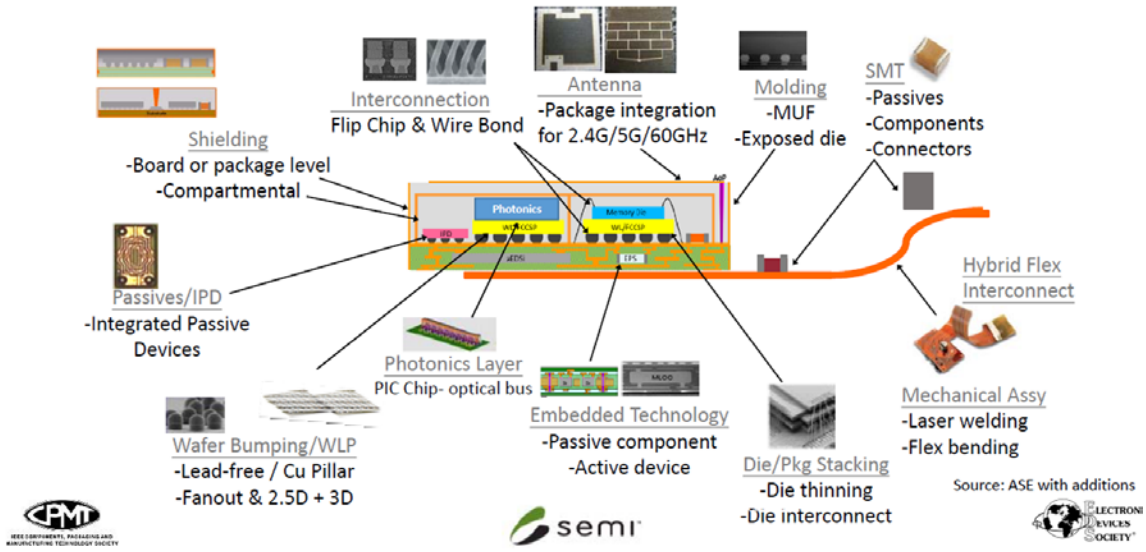

Figure 7 - Heterogeneous Integration is the integration of separately manufactured components into a higher assembly (SiP) that, in the aggregate, provides enhanced functionality and improves operating characteristics

In additional to performance enhancements, heterogeneous integration will enable a new paradigm, "functional disaggregation" which is a vital strategy to support trusted microelectronics. If we can fabricate individual chiplets in un-trusted fabs, we could then assemble them into a trusted micro-system. Each IP block can be instantiated as a partial function which by itself will not disclose the function of the system since the schematic (or block diagram) is incomplete. However, when all the chiplets are assembled and interconnected on the interposer, the complete schematic (i.e. function) is realized.

Therefore, the challenge for trusted heterogeneous integration technology is to stand up and maintain trusted 2.5D / 3D integration and assembly supply chain capabilities.

Programs such as DARPA CHIPS are leading the way for DoD contractors to explore, demonstrate and mature heterogeneous integration technology, design flows and re-usable IP blocks for future trusted microelectronics needs. Programs like DARPA SPADE are looking at disaggregation techniques for trust. Figure 8 shows the summary of future drivers, component solutions and critical trusted microelectronics issues for heterogeneous integration.

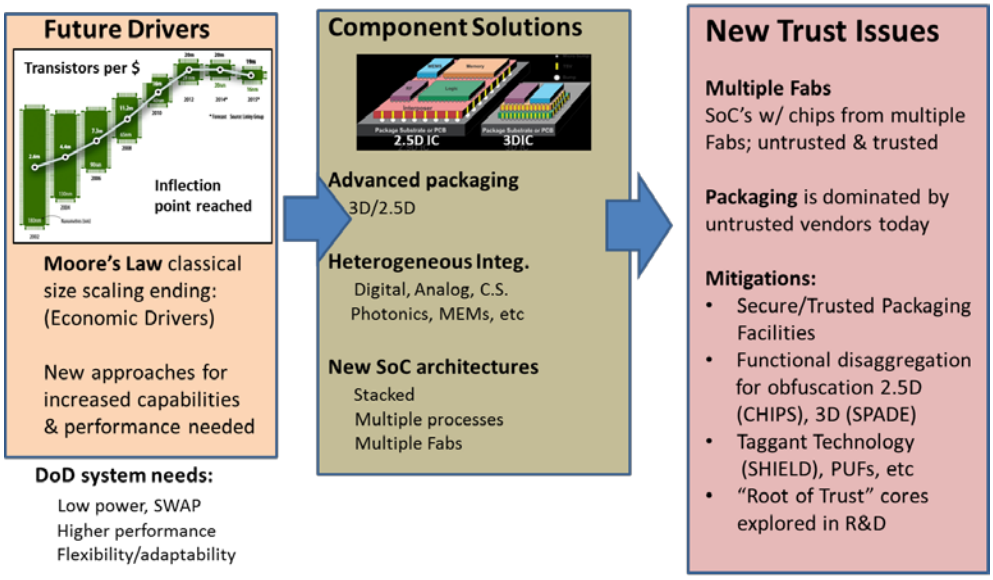

Figure 8 - Heterogeneous Technology Provides a Platform for Concurrent Development of Trust for Advanced DoD Computing Platforms.

5.2 Compound Semiconductor

The compound semiconductor industry has grown due to an increasing demand for robust high performance (power and frequency) RF military systems for ground, maritime and air and space. Although Silicon CMOS technology has continued to make great strides and demonstrate superior performance in various applications spaces for military systems, there are still limitations which have led to alternate technologies required to meet these specialized demands.

Over the last several decades, industry, academia and government have collaborated to deliver on the enhanced capabilities and performance potential of III-V wide bandgap material systems such as Indium Phosphide, Gallium Arsenide, Silicon Germanium, Silicon Carbide, Gallium Nitride, and Aluminum Nitride as well as recent work on ultra-wide bandgap compound semiconductors. Through DARPA funded programs (WBGS, DAHI NeXT, etc.,), collaborators have exploited the unique material properties of wide-bandgap materials and demonstrated record breaking and innovative achievements at the device, circuit, subsystem and system levels.

Despite the potential for enhanced performance of III-V compound semiconductors, the commercial sector has not generally adopted compound semiconductor technology for integration into consumer products. This is mostly due to their high cost and a lack of requirements for the high power and advanced capability offered. Gallium Nitride (GaN) on Silicon Carbide (SiC), for example, is not cost effective for consumer electronics when compared to silicon based RF technology. This is due to material complexity and cost.

However, certain sectors in the commercial market have transitioned to compound semiconductor technology replacing silicon technology, specifically in wireless mobile communication infrastructure (base stations), CATV, IoT, automotive and energy sectors. The performance benefits of higher power and better efficiencies have justified higher cost for compound semiconductor technology in certain application spaces. As availability of compound semiconductor material continues to grow, specifically GaN/SiC, costs will decrease and integration into consumers' systems will gain popularity. This will also be enabled by cost effective heterogeneous integration approaches discussed in the previous section. Figure 9 illustrates how these compound semiconductors have been adopted for military use, making them somewhat unique in the sense that the commercial markets lag DoD in their adoption.

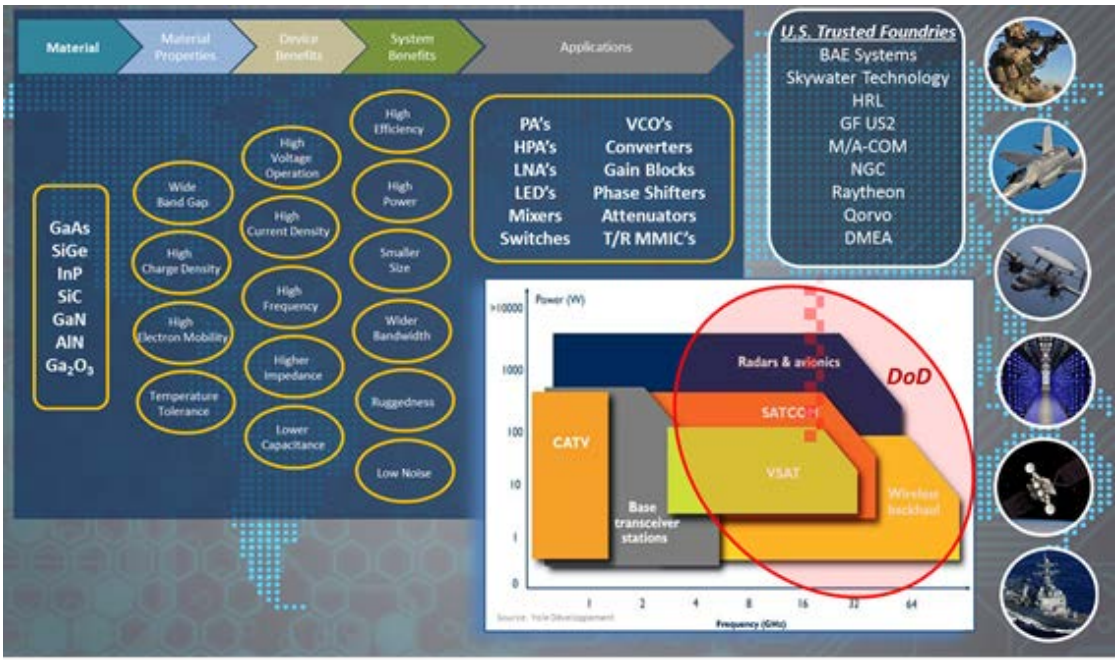

Figure 9 - Compound semiconductors play a crucial role in DoD systems.

As DoD continues to expand the performance envelope of military systems, the defense industry has and will continue to develop next-generation compound semiconductor-based electronics for military applications. In addition, compound semiconductor technology advancements from the commercial sector will also make their way to DoD systems in the form of state-of-the-art and inexpensive COTS products. The DoD will continue to focus on wide- and ultra-wide bandgap materials, keeping compound semiconductor technology as the workhorse to meet demanding future weapons systems requirements for the next 10-25 years. Because of this continued need, ***the existing industrial base must be protected*** as the commercial trajectory and cost versus performance model is likely going to remove the need for many of these legacy technologies in the supply chain.

5.3 Deep Node CMOS

The DoD requires access to state of the art (deep node) CMOS for a number of current applications as well as R&D efforts for future systems. Advanced node CMOS can provide compelling SWAP benefits for complex systems seeking to minimize their overall footprints. In addition, advanced digital computation requirements benefit tremendously from state-of-the-art (SOTA) CMOS solutions.

SOTA CMOS covers the realm of the very large and very small. The fabs involved are very large and expensive with high volume commercial facilities costing over $10B. R&D expenses are also enormous. For this reason, there are only 4 companies left that offer SOTA CMOS: INTEL, GLOBALFOUNDRIES, Samsung and TSMC. All of these companies rely on the scale of high volume manufacturing to finance the capital and R&D requirements to maintain their competitiveness. A figure summarizing the cost and suppliers of SOTA Fabs and their associated device technology is shown in Figure 10.

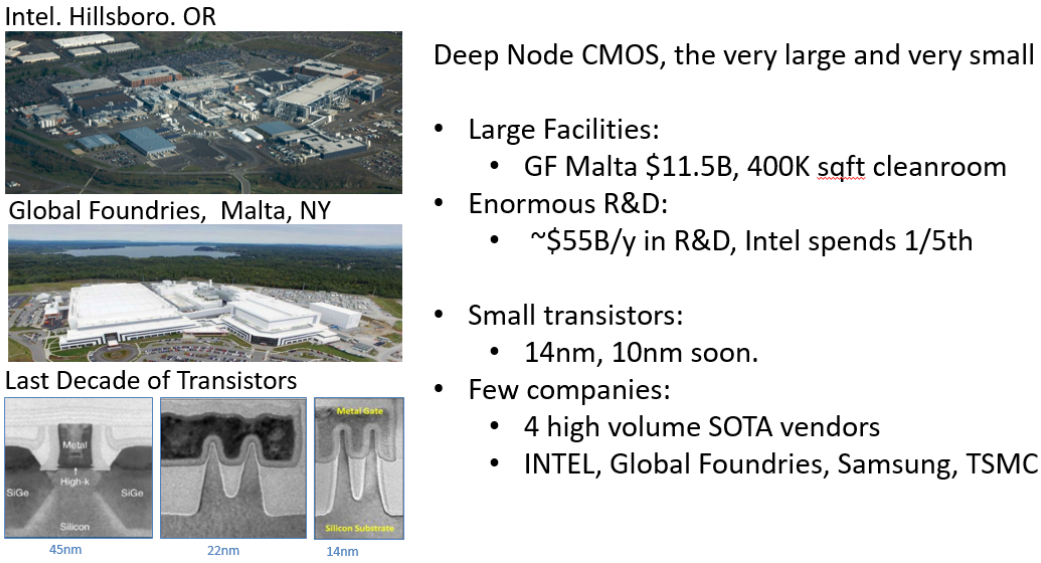

Figure 10 - Deep node CMOS provides many SWAP benefits using state of the art 14/16nm FinFETs.

As a result of the enormous cost and complexity of the SOTA CMOS business, DoD access has become very challenging in recent years. There is a substantial difference in business model for example with Industry needing to produce very large volumes of a small mix of parts over the short run while DoD requires substantially fewer parts across a broad device mix over the long run. The accelerating Non-Recurring Engineering (NRE) costs associated with SOTA design and fabrication make the high mix, low volume requirements difficult to attract commercial interest in servicing the DoD. This economic reality has encouraged the exploration of different engagement models. The

DoD has addressed this challenge in the past with its Trusted Foundry contract with IBM which ended in 2015 with the sale of IBM Microelectronics to GLOBALFOUNDRIES (GF), a foreign owned firm. The Trusted foundry contract managed by DMEA has now been novated to GFUS, a US subsidiary of GF.

In the long run, it is important for DoD to have assured access to secure SOTA CMOS from a variety of sources. Given the very different business models of the commercial world and DoD, this will be a challenging goal to achieve. The team has given some thought to this question and a number of potential pathways for achieving this are listed in Figure 11 below.

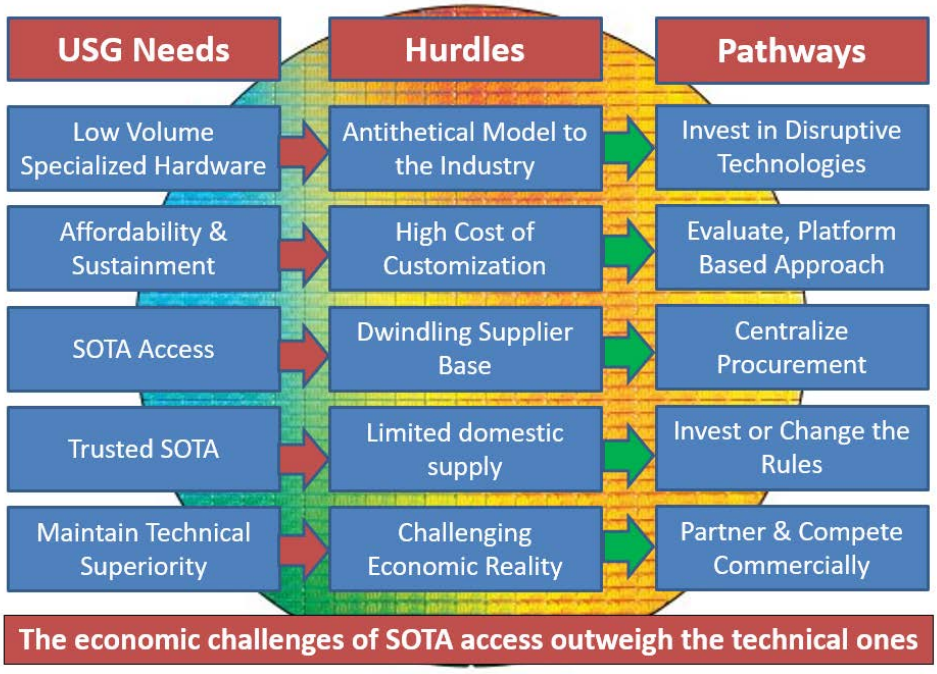

Figure 11 - Challenges and pathways for achieving DoD SOTA CMOS access

The DoD should be an early investor in disruptive new technologies thus gaining influence in these areas for the benefit of future DoD needs and helping ensure a healthy US Industrial base. Better aggregation of procurement should also be pursued building on the start the Trusted Access Program Office (TAPO) has made in this direction through the Trusted Foundry Program. The ideal case would be a whole of USG solution for access to SOTA components. The DoD should also consider revising or eliminating altogether some of the rules and red tape that invoke untenable business risks and discourage the commercial semiconductor world for working with them. Some areas requiring such reform include current acquisition policy, IP rights and ITAR for example. Finally, the best means for long term access to secure SOTA components should involve appropriate forms of public private partnerships with the commercial US semiconductor Industry. Completely captive production strategies for deep node CMOS are likely cost prohibitive. Developing win-win

relationships that benefit both commercial and USG parties in areas such as FEOL and BEOL, and others, should be investigated.

5.4 Other Emerging Technologies

One of the emerging technologies that may radically change the make-up, source, and development of microelectronics is that of advanced computing paradigms and approaches that diverge from simple transistor based logic and operations. This section looks at some of the aspects and, where possible, identifies any concerns that may arise within these new technologies.

With the looming end of Moore's Law, we are on the threshold of revolutionary new computing paradigms. Computing paradigms involve a framework of technology and science required to design and fabricate computing systems. The current paradigm of Von Neuman computing with CMOS components has had a long run of about 50 years. It has evolved as new technology and consumer demand resulted in more capability and integration of computing systems. The computer has evolved from performing batch operations to ultra-large scale network management functions toward smart, learning systems capable of autonomous, self-management. Figure 12 (following page) illustrates four emerging computing paradigms supported by a set of novel logic gate technologies. The complexity and scale of the component technology supporting new computing paradigms will bring greater challenge in hardware assurance and trust verification methods. Smaller feature size, unique gate architecture and very high gate counts present new challenges for reliability and cyber resiliency.

5.4.1 Advanced Digital Computing

Digital CMOS is currently at the 14 nm node with potential to scale to 3 nm by 2022. [6] The challenges with materials and process variation to achieve these new technology nodes drives increasing tool and fabrication costs, and renders a new concern for malicious insertions in the resulting complex design and fabrication flow. Alternatives for traditional silicon CMOS switches are being explored including spin-based logic, tunneling FETs and novel material FETs.

5.4.2 Analog Computing

Analog computing is receiving increasing attention with advanced SiGe RF technology, hybrid digital/analog platforms, NEMs, photonics and superconducting electronics. This paradigm is particularly well suited for emerging sensor applications and has significant power advantages for certain other applications as well.

5.4.3 Neuromorphic Computing

The Neuromorphic and Neuro-inspired computing paradigm is experiencing rapid growth with major companies having serious development efforts in this area (Google, Amazon, IBM, Microsoft etc.).

[6] http://www.eetimes.com/document.asp?doc_id=1330971

Current interests focus on machine learning and AI enabling applications. A key part of this development is the search for the optimum component hardware for efficiently implementing this paradigm. Some options currently being explored include FPGAs, custom IC's, resistive RAM, etc.

5.4.4 Quantum Computing

Quantum computing continues to be explored in efforts to take advantage of the large parallelisms possible for complex optimization and factoring problems. This will not replace conventional computing but potentially offer superior performance for certain specific applications.

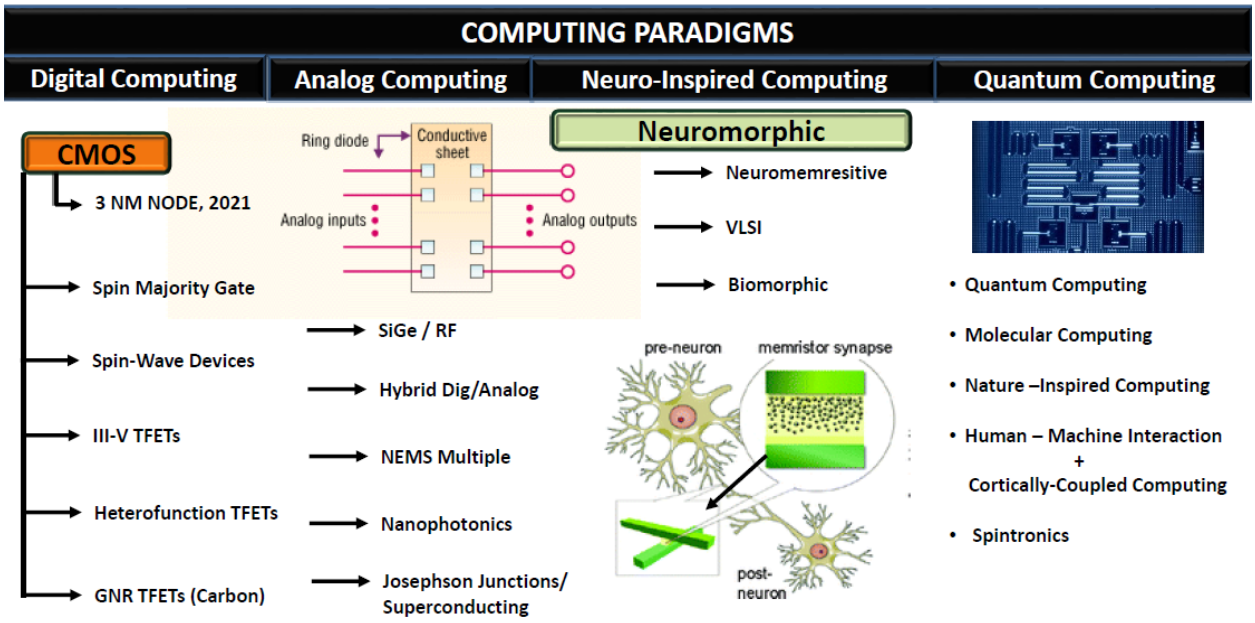

Figure 12 - Multiple technologies are going to revolutionize the world of computing over the next 5-10 years.

5.4.5 Advanced Research

Research organizations like DARPA and IARPA are working to achieve the concurrent breakthrough technology for instrumental analysis capable of studying the physics of failure in these new computing paradigms. This is a step toward malware characterization in evolving microcircuit technology used in novel computing paradigms. The same concern is evident for spintronic majority gate technologies, graphene-based Tunneling Field Effect Transistor (TFET) technology and other TFET technology. It is critical that work going on within the DoD and elsewhere, as it reaches viability, be kept accessible to the DoD as well as to the rest of US industries.

New computing paradigms will also create security challenges beyond the considerable ones already present with advanced CMOS and enumerated earlier. Analog computing, neuromorphic computing and quantum computing paradigms each involve alternative gate sets and architectures. Figure 13 shows the drivers and the embedded technology solutions enabling the new computing paradigms. The advancement of such emerging technologies will likely outpace industry's ability to understand the related security threats, and how to conduct appropriate vulnerability assessments.

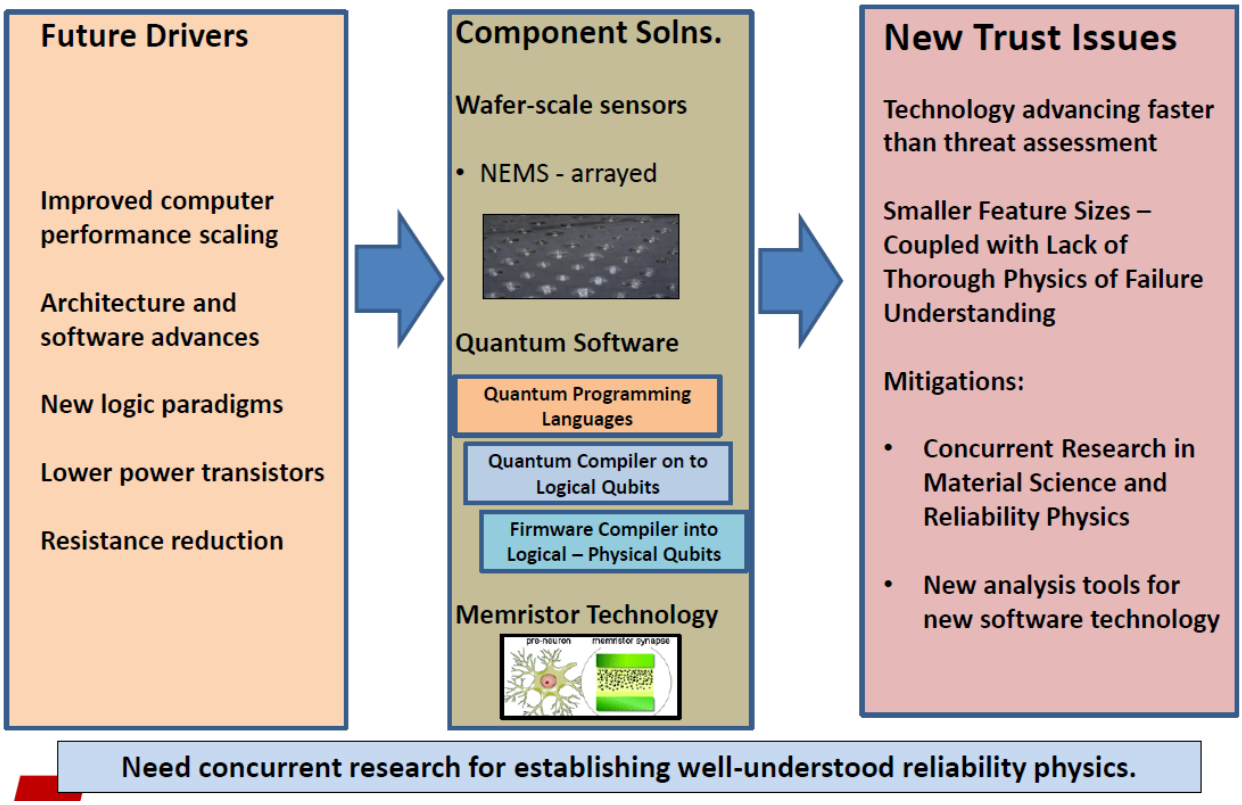

Figure 13. Future Drivers of Microelectronics Complexity and Supply Chain Trust Challenges.

Along with the introduction of new computing paradigms, the associated programming paradigms will be affected as well. For example, some parallel processing paradigms use qubit technology that does not act as conventional transistors. Instead, quantum computing uses quantum super-positioning to arrive at the most probabilistic answer. Such programming is one-step removed from the quantum equivalent of a logic gate. So, as shown in Figure 13, a programming paradigm is shown for Quantum computing that is distinct from traditional software paradigms.

The challenges presented by emerging computing paradigms call for new research in systems security engineering and secure circuit design methods. These methods should lend themselves to the generation of microcircuit IP, EDA tool design, operations security for the design and fabrication flows and sustainable assessment of hardware assurance over the life cycle of the microcircuit in its application.

6 SUMMARY OF FINDINGS AND RECOMMENDATIONS

This Joint Working Group consisted of Industry and Government Technologists, Engineers, and Executives with a good working understanding of the different ways Industry and Government "get things done". This experience has enabled us to look closely into the future of microelectronics and semiconductors for DoD systems over the next *10 years*. We examined 4 primary new and emerging technology spaces and discussed what concerns and challenges came to mind and what new mitigations to those challenges might be put in place.

- 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.

6.1 Key Recommendation

Create a National Microelectronics Strategy

While the US military global superiority and independence depends on eternal vigilance, our strength originates from constant technological innovation.

We have long prospered by allowing commercial entities the freedom to create and capitalize their products across all borders but with today's globalized world that freedom now jeopardizes our future if the Government does not plan an assured access strategy for the key microelectronic components it needs. Assured and secure access to emerging microelectronics technologies is a matter of national importance for the DoD as well as the US economy in general. The recent sales of

the IBM Trusted Foundry to foreign-owned GLOBALFOUNDRIES, along with other examples of the globalization of the semiconductor market, have driven home the point that we cannot afford to lose access to critical microelectronics component sources.

China is making very large investments in their microelectronics capabilities which will certainly impact the global market. Additionally, the risk from counterfeiting of microelectronics components (thoroughly described during the 2011 Senate Arms Services Committee hearings) [7] grows each day. Given the importance of this, a National Strategy to achieve assured secure access to microelectronic technologies throughout a defense systems' lifecycle is an imperative in our opinion.

This team is advocating and recommending that a National Microelectronics Strategy be created that includes a 10 year plan and supporting budget for achieving assured access to advanced microelectronics technologies.

We recommend that this Strategy emerge from the DoD as the key microelectronics equity within the USG. It is our belief that the Strategy, once in a framework, should then be vetted and coordinated across all of Government (including DoE, DoD, the IC, Commerce, HS, etc.). Implementation will also require coordination with the Industrial base and State governments.

The DoD is best positioned take the lead in creating and building momentum for a strategy that once defined, will be first and foremost about protecting the United States and its interests. Such a strategy is needed for both National Security and Economic Health of the US. We currently have about 50% of the worldwide semiconductor market and Microelectronics are the #3 export of the US. The National Security and economic stakes are simply too high for a National Strategy not to be implemented for this critical area.

Specific Additional Sub-recommendations for Leading Edge and Emerging Microelectronics Technologies: Each of the following sub-recommendations can be considered as viable components of a National Microelectronics Strategy or as independent actions:

6.2 Sub-recommendation 1: PLAN and ACT

Be Proactive as part of a Strategy

Track Future Technology Trends & Impacts: Look ahead 10 years based on system and concept trajectories today to identify today's emerging innovators, technologies, solutions, and concepts as well as emerging adversaries, risks and threats across all of electronics-based systems. This focused tracking of futures "on the radar" will dramatically improve outcomes as government will have time to be proactive when warranted and reactive when necessary.

[7] https://www.armed-services.senate.gov/press-releases/senate-armed-services-committee-releases-report-on-counterfeit-electronic-parts

Exchange investment for access: New technology is often inspired, encouraged and/or enabled by US or State Government entities at its inception when commercial risks are high. Build in long-term access plans for the government as part of such investments. Early engagement in new technologies (like 3DIC, neuromorphic, etc.) may help ensure both access and a healthy US Industrial base in these emerging areas.

Encourage Investment and Transition: Enable a robust environment for transitioning R&D results into US production such as secure 3D/2.5D integration facilities. Work to establish centers of excellence for bringing new technologies across the "valley of death" into commercial US deployment and into the hands of the warfighter. This will require judicious investment and coordination across state, federal, university, entrepreneurs and large industry players.

Organize for the Future: Create collaborative government-industry-academia microelectronics entities for future trust and assurance capabilities. This should be made easier by centralizing this strategy and ownership across the USG. Establish effective public private partnerships to help bridge the cultural and technology gaps between US Industry and DoD. Also, develop a more attractive government microelectronics market through better aggregation of demand and resources. The Industry, OSD MIBP and the Department of Commerce have taken great strides to assess the market, ***and now centralizing/organizing this effort is critical for our success.***

6.3 Sub-recommendation 2: PROTECT and COORDINATE

Obtain protections for entire microelectronics supply chain throughout the system lifecycle by creating a dynamic "web" of solutions for best protection

Expand Trust and Risk Mitigation for ALL USG: Develop a whole of USG approach that aligns major entities concerned about trusted and assured microelectronics (DoD, DOE, IC, DOJ, etc.). As part of this approach, combine Cyber, Trust, and Anti-Tamper Silos into a Unified Risk Mitigation Strategy.

Also:

- Explore "design for trust" methods, verification/forensics, obfuscation, metrics, re-configurability, etc.
- Develop spectrum or "tiers" of trust levels/categories and adapt source selection practices to consider acquisition phase through sustainment.
- Build broad portfolio of trusted and trustable suppliers, ranging from cleared contractors to commercial vendors that adhere to trust practices.

Connect and Build with Existing Innovators and Solutions: Semiconductor industry innovations will provide great national defense benefits if properly adapted and integrated into more complex DoD

systems. A National Strategy should leverage the global semiconductor industry and incentivize these profit driven entities to innovate, manufacture, and invest in the US semiconductor industry.

By utilizing commercial building blocks and testing to well-defined risk standards, a National Strategy will adapt/augment commercial microelectronics to create a strategic or tactical edge over near peer countries. The decision to test or modify the commercial components will depend upon each program/mission to ensure that "augmented COTS" is superior to vanilla COTS that an adversary may be using.

Protect assured access to legacy technologies: While Nationalized deep node CMOS foundries may not be the answer; there are specific areas of concern with trusted and assured access to technology particularly SOTA. Partnerships with industry are therefore imperative, but assured access, and transfer and retention of US Intellectual Property is key. We do feel that there is need for some nationalized strategy, and especially USG defined and centralized leadership for microelectronics.

Offer Umbrella of Protection to all Industries: Connect with non-defense industries that may have an interest in trusted and assured microelectronics (automotive, banking, medical, etc.)

6.4 Sub-recommendation 3: REACT and EXTEND

Good planning and strategies should include reaction to unforeseen changes and uncontrollable events

Establish Fast-Follower Technology Adoption – Things built for commercial use may be more easily adopted and adapted to DoD and other critical infrastructure usage through rapid adoption strategies, many of which are in play across USG but a National Microelectronics Strategy should enable coordination of these disparate strategies.

Provide Current Data to CFIUS and other Acquisition-mitigation entities: *What new technology can we not afford to lose?* Being able to assemble data about single source solutions quickly will take coordination across all USG entities.

Expect Surprises - Create Contingency and Rapid Reaction Plans: The best planning does not anticipate everything or prevent all failures. Setbacks are inevitable and if the past is any evidence, a core strength of our country is the ability to innovate and solve problems under pressure. A critical component of a National Microelectronics Strategy is to avoid high cost for low risk mitigations. A rapid reaction strategy will be far more economical and politically viable than to protect against all possible negative outcomes.