NDIA

Trusted Microelectronics

Joint Working Group

Team 2 White Paper:

Trustable Access to Leading Edge Technology

June 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. 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]

This paper examines the challenges posed by the USG's unique requirements and low volume demand and presents a number of options for addressing cost pressures that currently affect the USG's continued access to leading edge technologies. At the same time, continued investments in R&D and manufacturing infrastructure could bolster the domestic commercial semiconductor industry, to the benefit of public and private sector purchasers.

The need could not be more urgent. The growing sustainment and modernization challenges for USG systems continue to increase, largely due to electronics parts obsolescence, access barriers to advanced technologies, and long USG system lifecycles with a low rate of technology refresh. Additionally, other nations do not impose similar trust restrictions on themselves and are investing very heavily in building semiconductor capabilities, including those at the leading edge such as advanced commercial tools, semiconductor processes, components and electronics. Through such measures, U.S. adversaries potentially could gain the warfighting edge.

Addressing these issues requires broad collaboration, not only within the government, but between government, industry and perhaps other countries. To stay ahead in warfighting capabilities for national security and increased economic prosperity, the United States needs an economic and

[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"

policy environment that fosters innovation in semiconductors, especially in leading edge semiconductor technology nodes. The PCAST report (Jan 2017) also addressed the rise of China's semiconductor industry and recommended that the United States improve its environment for development of the semiconductor and high-tech industries and continue to invest in advanced technologies. Time is of essence to take bold meaningful steps to ensure American technical superiority and national security advantage.

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.

III. PRINCIPAL CONTRIBUTORS

The team was composed of 28 dedicated team members from 20 organizations who all contributed diligently to this work.

Name	Organization
Adam Hauch	Defense Security Service
Aman Gahoonia	Defense Microelectronics Activity
Anita Balachandra	TechVision21
Brad Botwin	Department of Commerce
Brett Attaway	AIM Photonics Institute
Brian Cohen	Institute for Defense Analyses
Christine Rink	The Aerospace Corporation
Dan Radack	Institute for Defense Analyses
David Gottfried	Alfred University
David Pentrack	Defense Microelectronics Activity
Doug Palmer	Booz Allen Hamilton
Erika Maynard	Department of Commerce
Ezra Hall (Team Leader)	**GLOBALFOUNDRIES**
Gerry Borsuk	Naval Research Laboratory
Gerry Etzold	Etzold Technology Consulting
James Chew	Cadence
Jeremy Muldavin	Office of the Deputy Assistant Secretary of Defense for Systems Engineering DASD (SE) Microelectronics Assurance
John Verwey	Department of Commerce
Kelly Hennig	Northrop Grumman
Mark Crawford	Department of Commerce
Michael James	IBM Global Business Services
Neal Levine	Defense Microelectronics Activity
Neil Schumacher	IBM Global Business Services
Paul Syers	Potomac Institute for Policy Studies
Peter Wheatley	Department of Defense
Taffy Kingscott	IBM
Tyler Schmidt	Intel Federal
Vashisht Sharma	Institute for Defense Analyses

IV. SOURCES

This is a list of sources used as references but are not otherwise identified or cited elsewhere within this document.

Table 1 – List of Non-cited References

Analysis, Institute for Defense. 2014. Chinese Microelectronics and Computing Technology – 2014 Update. Alexandria, VA: Institute for Defense Analyses.

Analysis, Institute for Defense. 2016. *State of the Defense Microelectronics Industry.* Alexandria, VA: Institute for Defense Analyses.

Commerce, U.S. Department of. 2015. *2015 Top Markets Report Semiconductors and Semiconductor Manufacturing Equipment.* Washington, DC: U.S. Department of Commerce.

Commerce, U.S. Department of. 2016. *2016 Top Markets Report, Semiconductors and Related Equipment.* Washington, DC: U.S Department of Commerce.

Commerce, U.S. Department of. 2010. *Defense Industrial Base Assessment: Counterfeit Electronics.* Washington, DC: U.S. Department of Commerce.

Commerce, U.S. Department of. 2016. "The U.S. Semiconductor Industry and Imapcts of China's Semiconductor Policies." *GOMACTECH 2016* 14.

Commerce, U.S. Department of. 2016. "U.S. Department of Commerce Bureau of Industry and Security." *GOMACTECH 2016* 12.

Commerce, U.S. Department of. 2009. *U.S. Integrated Circuit Design and Fabrication Capability.* Washington, DC: U.S. Department of Commerce.

Cotton, Tom (United States Senator). 2016. "Letter to Armed Services, Banking Housing and Urban Affairs, Joint Economic Committee, Selecf Commitee on Intelligence, Special Committee on Aging." *Letter to the Honarable Ashton Carter, Secretart of Defense.* Washington, DC, April 8.

Service, Congressional Research. 2017. *U.S. Semiconductor Manufacturing: Industry Trends, Global Competition, Federal Policy.* Washington, DC: Congressional Research Service (www.crs.gov).

Studies, Potomac Institute for Policy. 2016. *Hardware and IP Security in the Commercial World.* Arlington, VA: Potomac Institute for Policy Studies.

(This Page Intentionally Blank)

V. TABLE OF CONTENTS

VI. LIST OF FIGURES

1 EXECUTIVE SUMMARY

The NDIA convened a joint working group, composed of industry, government, and academic representatives, to examine pressing issues regarding USG[2] access to trustworthy microelectronics. A sub-group chose to examine the challenges of maintaining access to trusted sources of State-of-the-Art (SOTA) microelectronics. In this paper, the team addresses 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 proposes 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 actions, 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]

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.

[2] For the purposes of this discussion, USG refers to the federal agencies with a national security mission, i.e., the Departments of Defense and Energy (NNSA) and the Intelligence Community. The term "public sector" refers to functions that are inherently public (such as electric utilities), but may be executed by federal, state, local or private non-profit entities.

[3] For more information on effects, see the 2015 GAO report *Trusted Defense Microelectronics: Future Access and Capabilities are Uncertain* and the 2016 Potomac Institute for Policy Studies report Ensuring Access to Trusted State-of-the-Art Microelectronics.

- 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 Trust4 (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.

2 INTRODUCTION

As part of its efforts supporting the Trusted Microelectronics community, NDIA convened a joint working group, composed of industry, government, and academic representatives to examine a number of pressing issues regarding USG access to trustworthy microelectronics. The larger joint working group formed four targeted teams, each to examine a major issue facing the community. This paper addresses the challenge of maintaining USG access to trusted sources of SOTA microelectronics.

Three key questions formulated the basis for this team's effort.

[4] http://www.dmea.osd.mil/trustedic.html

JWG Team 2 Questions:

1) **Consequences:**
What are the potential consequences of the Chinese Government's substantial global semiconductor investments to the U.S. commercial and defense microelectronics industrial base?

2) **Impacts:**
What are the economic and national security implications of losing access to reliable U.S. and non-U.S. foundries, manufactured components, equipment, intellectual property, and know how, for both commercial and Trusted handling levels?

3) **Actions:**
What actions (USG, public sector as whole, and Industry) could be taken to stabilize and sustain the U.S. defense microelectronics industrial base?

Six sub-teams created the content in this report, structured according to the categories

(1) Consequences, (2) Impacts, and (3) Actions.

JWG Team 2 consisted of the following Sub-Teams:

- 21st Century SoCs
- End-to-End Education
- Acquisition Reform
- National Policy and Public-Private Partnerships
- Aggregation Models
- Trust Models
    - 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.)

3 BACKGROUND

3.1 Semiconductor Fabrication Process

The semiconductor fabrication process encompasses a wide diversity of domains to enable an End to End Microelectronics Workflow (E2E Flow) that produces the electronic devices we all utilize in our daily lives. Figure 1: End-to-End Microelectronics Workflow (E2E Flow) illustrates the major stages of both hardware and software development involved in creating SOTA microelectronics that are ubiquitous in modern systems. It is important to note the process illustrated here occurs at geographically disparate locations, across multiple companies and countries. This especially holds true in SOTA technologies, where highly specialized skills, facilities, and vendor support are required for each E2E Flow element.

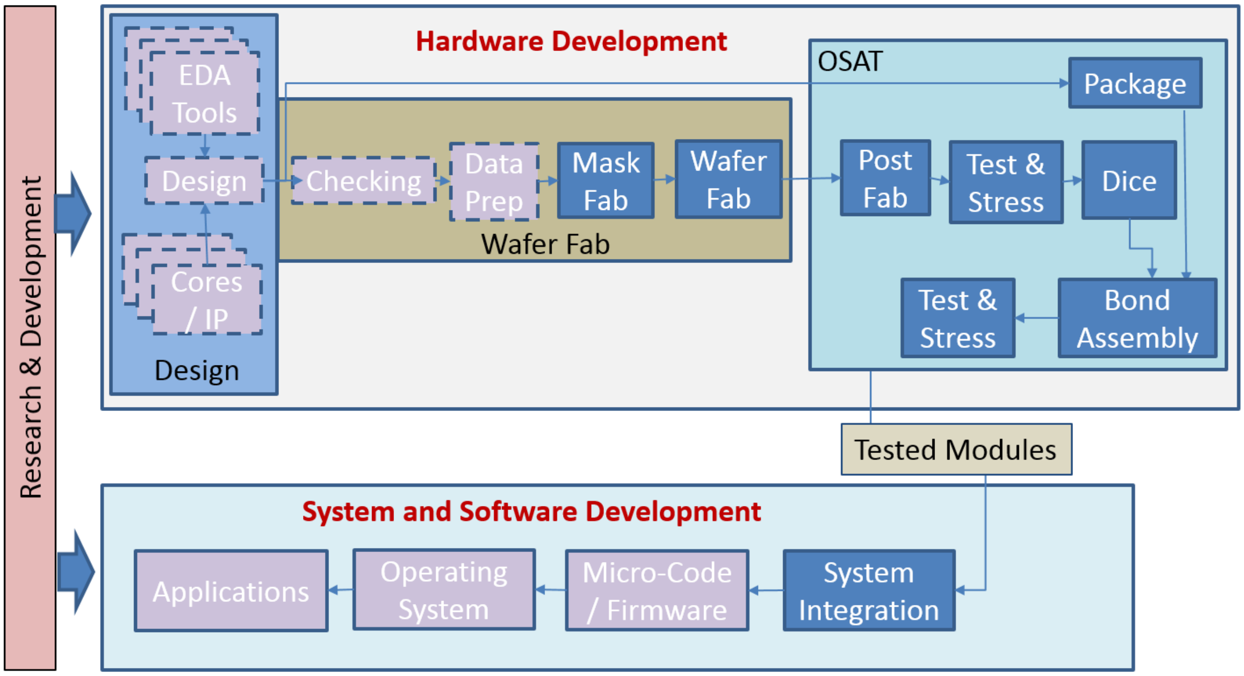


Figure 1: End-to-End Microelectronics Workflow (E2E Flow)

The major stages that make up this E2E Flow are:

- **Fundamental research and development** creates the technologies utilized in each step of this flow. Continued USG investment in such foundational research is necessary to enable continuous innovation in the U.S.
- **Hardware Development** which is further sub-divided into stages:
    - **Design** implements and expresses the architectural functionality necessary to create a semiconductor device that performs the required functions. This can span functionality from power amplifiers, to sensors, to memory, processors for data manipulation and High Performance Computing (HPC) analysis. Industry standard Engineering Design Automation (EDA) tools are utilized for this work, and are enabled with the Intellectual Property (IP) from ecosystem vendors, and technology specific enablement from a foundry.
    - **Wafer Fab** is the process of taking the design data file from the customer, manipulating that data to create photolithographic masks that express the design into its individual levels, and then using those masks to fabricate semiconductor wafers that function according to the design file.
    - **"OSAT"** is **o**ut**s**ourced **a**ssembly and **t**est, where each wafer is tested and individual product dies are bonded to package substrates to create larger assemblies called modules, which are shipped to the system integrator.
- **System and Software Development** which incorporates the semiconductor chips (typically in module form) and combines them with discrete components on Printed Circuit Boards (PrCBs), along with firmware and software, to create working system level circuit boards.

4 CONSEQUENCES

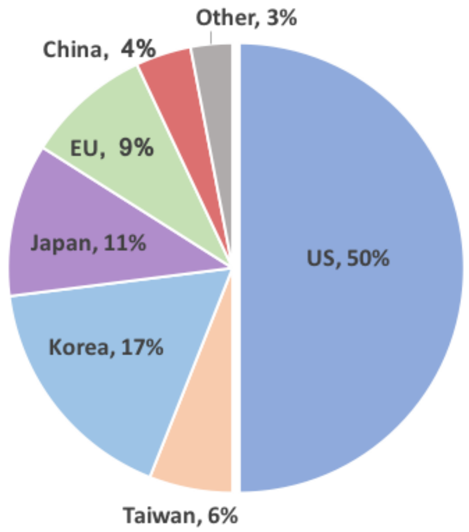
4.1 Global Semiconductor Market

Today the U.S. is the global leader in semiconductor revenue. However, a comparison of individual company revenue obscures a growing weakness of the U.S. semiconductor industry. While the U.S. claims slightly under 50% of global sales[5] (see Figure 2: Global Market Share (Sales)), and U.S. companies lead in revenue in critical areas, only approximately 20% of planned new worldwide capacity is under U.S. ownership in 2017-18 (see discussion on page 8). Furthermore, the U.S. share of total worldwide fab capacity had fallen to ~13% in 2015, (see Figure 3: Global Wafer Fabrication Capacity) down from 30% in 1990 and 42% in 1980[6] for 300mm wafer size technologies (SOTA). This separation of revenue from fab capacity is due to the growing trend of semiconductor companies

[5] http://trade.gov/topmarkets/pdf/Semiconductors_Executive_Summary.pdf

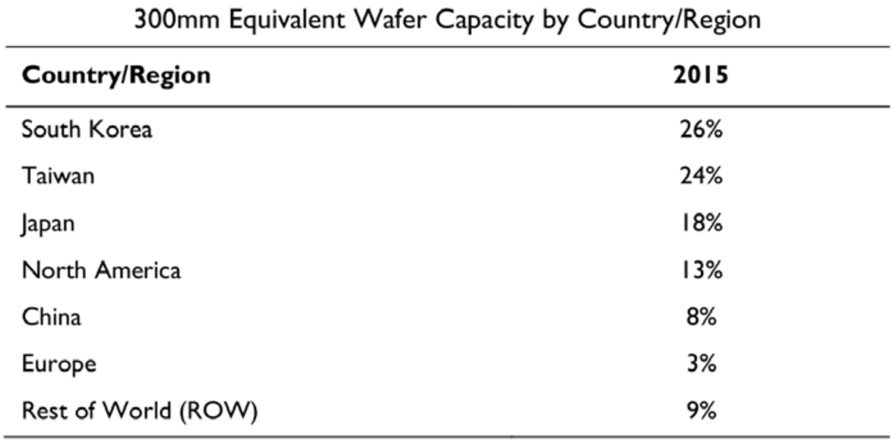
[6] https://fas.org/sgp/crs/misc/R44544.pdf

becoming "fabless," a model of operation wherein companies design products and outsource fabrication to pure play foundry semiconductor suppliers.



Source: SIA-World Semiconductor Trade Statistics / IHS/PwC/IC Insights
Share based on headquarters of seller: foundry output not included, fabless included.

Figure 2: Global Market Share (Sales)



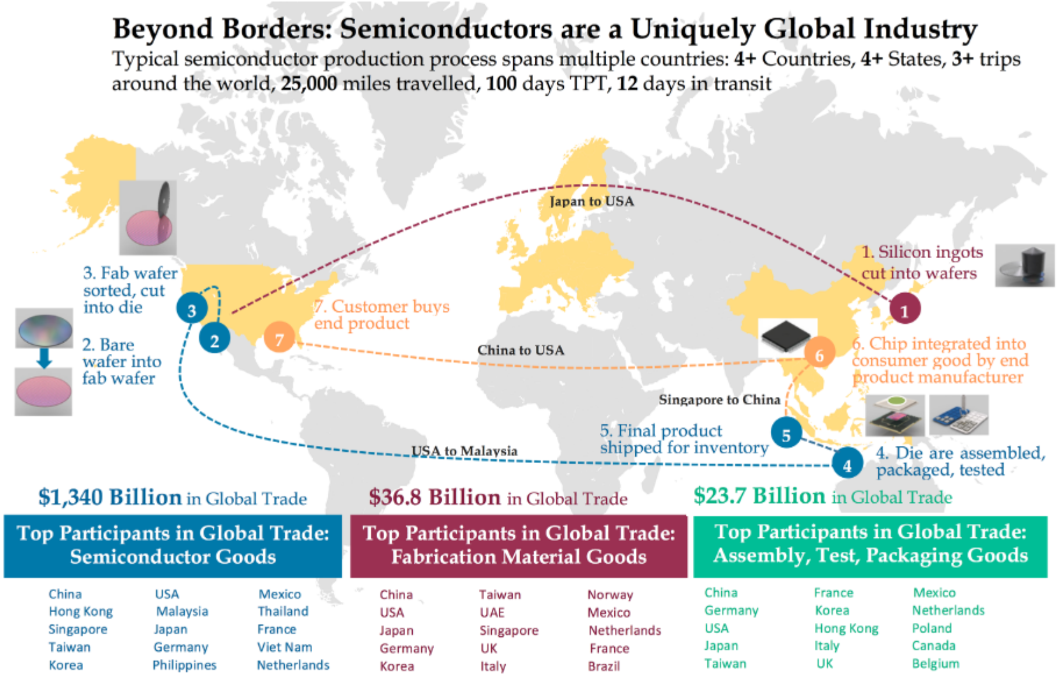
300mm Equivalent Wafer Capacity by Country/Region

Country/Region	2015
South Korea	26%
Taiwan	24%
Japan	18%
North America	13%
China	8%
Europe	3%
Rest of World (ROW)	9%

Source: *U.S. Semiconductor Manufacturing: Industry Trends, Global Competition, Federal Policy*, June 27, 2016, Congressional Research Service

Figure 3: Global Wafer Fabrication Capacity

One possible representative sequence of operations for a product is depicted in Figure 4: Commercial Semiconductor Foundation.[7] Many workflows occur, each finely tuned to supplier availability and the unique needs of a particular product. For example, assembly and test operations have largely migrated to Asia as the world-wide center of competency for such work.



Beyond Borders: Semiconductors are a Uniquely Global Industry

Typical semiconductor production process spans multiple countries: **4+** Countries, **4+** States, **3+** trips around the world, **25,000** miles travelled, **100** days TPT, **12** days in transit

Japan to USA
1. Silicon ingots cut into wafers
1
3. Fab wafer sorted, cut into die
3
2. Bare wafer into fab wafer
2
7. Customer buys end product
7
China to USA
6. Chip integrated into consumer good by end product manufacturer
6
Singapore to China
5. Final product shipped for inventory
5
USA to Malaysia
4. Die are assembled, packaged, tested
4

$1,340 Billion in Global Trade

Top Participants in Global Trade: Semiconductor Goods

China
Hong Kong
Singapore
Taiwan
Korea
USA
Malaysia
Japan
Germany
Philippines
Mexico
Thailand
France
Viet Nam
Netherlands

$36.8 Billion in Global Trade

Top Participants in Global Trade: Fabrication Material Goods

China
USA
Japan
Germany
Korea
Taiwan
UAE
Singapore
UK
Italy
Norway
Mexico
Netherlands
France
Brazil

$23.7 Billion in Global Trade

Top Participants in Global Trade: Assembly, Test, Packaging Goods

China
Germany
USA
Japan
Taiwan
France
Korea
Hong Kong
Italy
UK
Mexico
Netherlands
Poland
Canada
Belgium

Figure 4: Commercial Semiconductor Foundation

This shift is largely the outgrowth of a truly global industry with a global value chain. Whereas the industry was originally highly vertically integrated, over the past several decades the commercial E2E Flow has become segmented, with companies specializing in particular market niches. Thus, the semiconductor industry increasingly operates on a global basis in which work on a single product is performed at locations all over the world by multiple companies specializing in their respective areas of expertise.

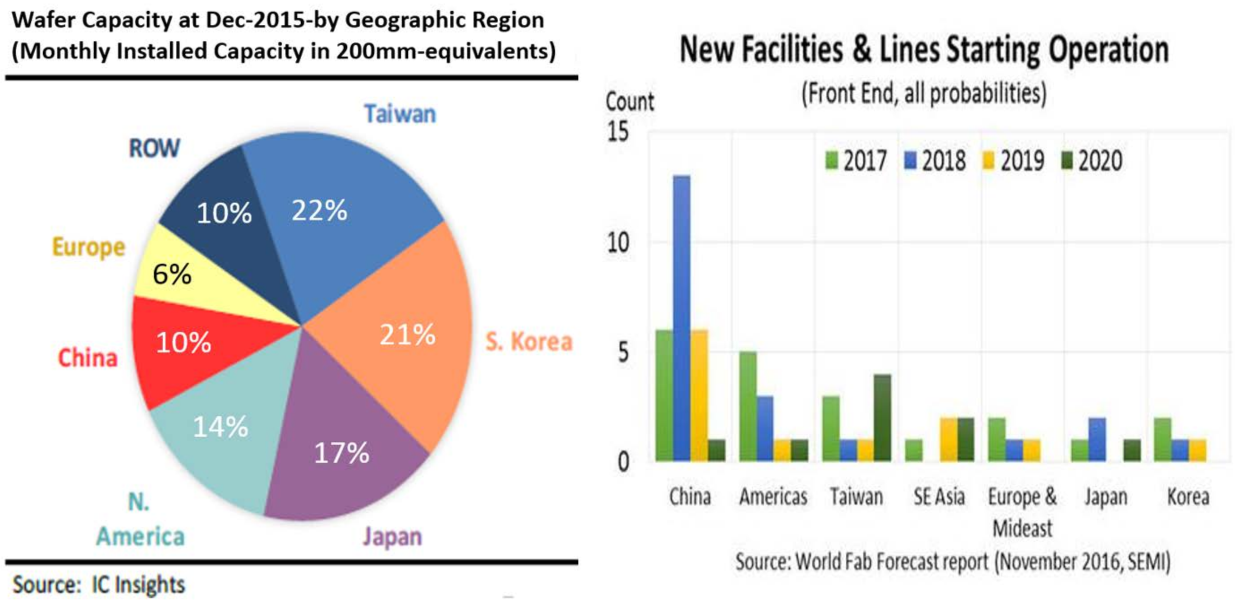
Additional insight into future regional *availability* of semiconductor supply can be gleaned by analyzing announcements for new fabs by region (see Figure 5: Wafer Fab Trends[8,9]). While some announced fabs may not ultimately be built, it is notable that announced fabs for construction in China (26) vastly outnumber any other region, including the Americas (10), by more than 2.5X. Such

[7] https://www.semiconductors.org/news/2016/05/06/press_releases_2016/new_report_highlights_benefits_impact_of_global_semiconductor_value_chain/

[8] **http://www.icinsights.com/news/bulletins/20152016-Deals-Dominate-Semiconductor-MA-Ranking**

[9] http://www.semi.org/en/fab-investment-surge-china-0

increased capacity in China would bolster technology *availability* to that region, create the potential for oversupply and would place significant market pressure on suppliers in the rest of the world, including the U.S.


Wafer Capacity at Dec-2015-by Geographic Region (Monthly Installed Capacity in 200mm-equivalents)

New Facilities & Lines Starting Operation (Front End, all probabilities)

Source: IC Insights

Source: World Fab Forecast report (November 2016, SEMI)

Figure 5: Wafer Fab Trends

The offshoring of crucial components and processes is not new; in fact, globalization of production has been occurring for decades. In the 1970's and 1980's both Japan and Taiwan grew their domestic semiconductor industries substantially with significant government support. In the 1980's the U.S. responded to Japan's actions in the market by supporting increased domestic innovation in strategically significant activities. Sematech, a pre-competitive research consortium, was created and funded jointly by the industry and the DoD to recapture the leading edge in semiconductor equipment manufacturing.

Today, China is attempting a similar transformation, but on a much larger scale. While the pace of production innovation has traditionally made it difficult for countries to gain dominance quickly over established players in SOTA semiconductor production, the industry is changing in fundamental ways that make it easier for a country like China to close the technology gap in a matter of a few years, especially if it provides strong support at the national, regional and local levels, which it currently plans to do.

5 IMPACTS

5.1 Economies Of Scale

The semiconductor industry has grown from less than $50B in annual revenue in 1987 to over $350B in 2016, with a current rate of year-on-year growth of approximately 3.5%, down from 22% in the 1980s when the industry was much smaller. [10] However, the pace of technology innovation, while somewhat slowed, continues to place pressure on SOTA market leaders. This pressure derives from the scaling and innovation challenges associated with shrinking transistor size and commensurate growth of density and performance to achieve lower per unit costs with greater functionality. This progress, however, has come at a substantial increase in the upfront cost of design, masks, packaging, and testing.

The first result of this pressure is that fewer and fewer companies can realize a viable business case for investing at the levels necessary to compete with the most advanced technologies. This began to have a dramatic effect on the industry at the 90nm technology node, when fewer and fewer companies could justify the investment based on their available markets. Many companies chose to remain at older nodes and find a market niche, or abandon the manufacturing portion of their business by engaging in the fabless semiconductor foundry model. Industry analysts predict that at 14-16nm only four companies will maintain leading edge manufacturing capabilities. Companies may merge with or acquire other companies (Mergers and Acquisitions (M&A)) to increase their available market size to remain profitable in the face of increased costs. In 2015, the semiconductor industry saw an unprecedented worldwide M&A volume of more than $125B. This consolidation is a strategy to increase scale, leverage R&D, and become more competitive.

Figure 6: Industry Consolidation (page 10) illustrates how this consolidation and movement to the foundry model has affected companies as they strive to justify the business case for more advanced technologies. While the most vivid example of this is the four companies that manufacture at 14-16nm nodes, the same dynamic characterizes the entire industry. This chart is just a snapshot in time; some companies that currently compete at 45 or 32 nm may choose to consolidate or exit the semiconductor manufacturing business and become fabless in the future.

These economies of scale also apply to other segments of the supply chain, where similar waves of consolidation have been observed. Fabless companies have consolidated, as have some of the semiconductor equipment suppliers. Large and familiar brands like Broadcom (Avago), SanDisk (Western Digital), Altera (Intel), Freescale (NXP), and KLA-Tencor (Lam Research) have been absorbed by even larger companies (listed in parentheses). China's ambitions to grow quickly its indigenous semiconductor supply chain have contributed to this trend. Recent acquisitions by Chinese companies include ISSI, OmniVision, NXP RF power unit, and, notably, Mattson in the semiconductor equipment segment.

[10] www.statistica.com/statistics/2669731/

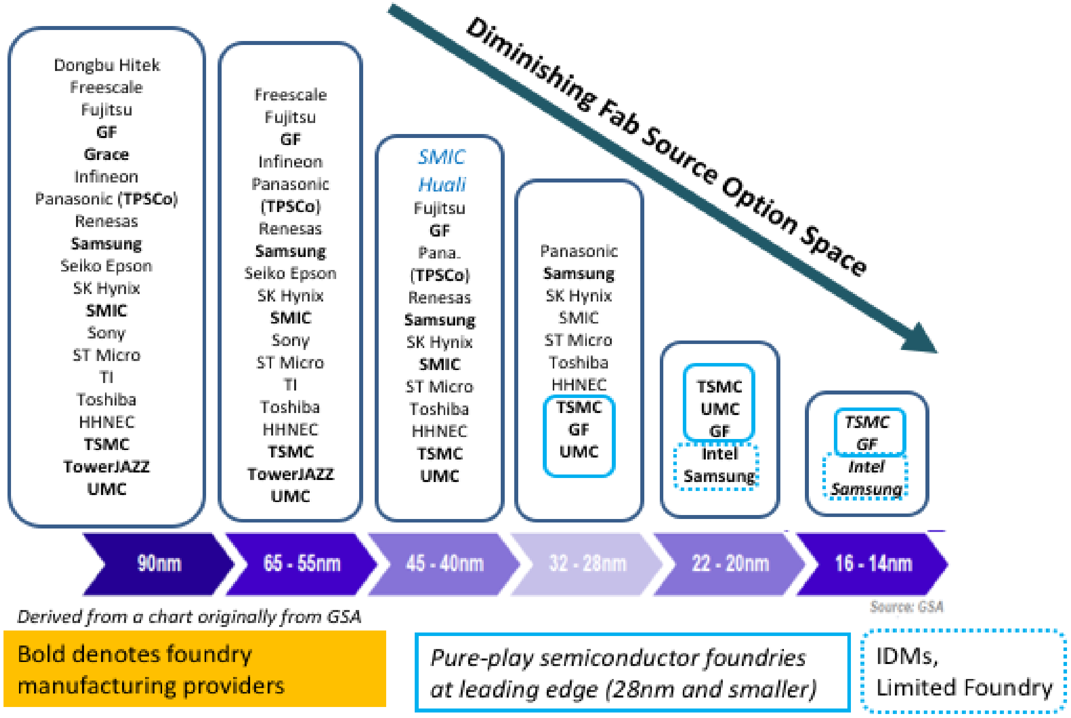


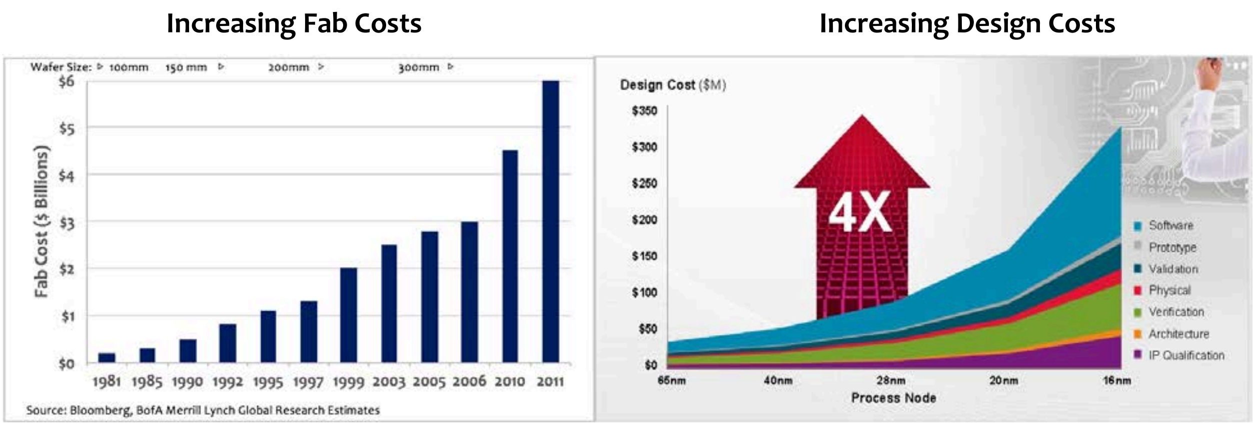
Figure 6: Industry Consolidation

To understand the pressure on the semiconductor manufacturing segment of the business, consider that just a decade ago, an advanced semiconductor fab cost about $2B to $3B. Today, that number has grown significantly, with Samsung announcing in May 2015 that it was breaking ground on a fab that will cost $14B[11]. The technologies in these fabs are often only financially viable for 5-10 years before newer technologies dominate and overtake demand, so the business case for the fab must be satisfied in that fairly short timeframe. As a whole, industry invests only about 18% of revenue in new fabs, and similar economics govern the development of new products. As a result, only those companies that can produce high volumes of products sold at a significant profit can economically justify the investment required to build the most advanced semiconductor fabs. At the moment, Samsung and Intel are the sole Integrated Device Manufacturers (IDMs) with advanced fabs. The rest of the industry relies upon sourcing from pure play foundries, of which there are two at the leading edge, TSMC and GLOBALFOUNDRIES. Samsung, Intel and GLOBALFOUNDRIES are on-shore, while TSMC is off-shore.

To understand these processes, consider manufacturing runs as the production of a single product on a selected fab process. Typically, there are several products that support very high volume runs such as the core semiconductors in mass consumer products like smartphones, tablets, and PCs.

[11] http://www.eetimes.com/document.asp?doc_id=1326565

These high volumes and large manufacturing runs amortize the large fixed costs of product development and fab operation over large quantities. The situation changes, however, with smaller manufacturing runs and for fabs that generate small volumes of production. Advanced semiconductor companies consider anything below millions of units as "small." Small runs have fixed costs, sometimes called Non-Recurring Expenses (NRE), associated with development of each product. Those NRE costs include tasks such as design, mask fabrication, test, qualification, and yield ramp-up. As shown in Figure 7: Dramatic Rise in Fab and Design Costs, design cost, in particular, has been increasing dramatically. Total NRE development costs for new products at 32 nm, for example, projected to be as much as $100 million. Commercial businesses often amortize such up front NRE across production parts, on a per unit basis, spreading the cost over volume. If a product's production lifetime volume consists of 10 million units, then a $100 million fixed cost, allocated across the production lifetime volume, would add $10 to each unit. But a typical production lifetime volume for USG purposes may only be 10,000 units, which means that NRE effectively adds $10,000 to each unit's cost. That economy of scale drives a model in which NRE costs dominate total program costs for low volume USG uses, causing them to become prohibitively expensive in SOTA technologies. This concept is further explored in the section "USG Misalignment with Commercial" below.


Increasing Fab Costs

Increasing Design Costs

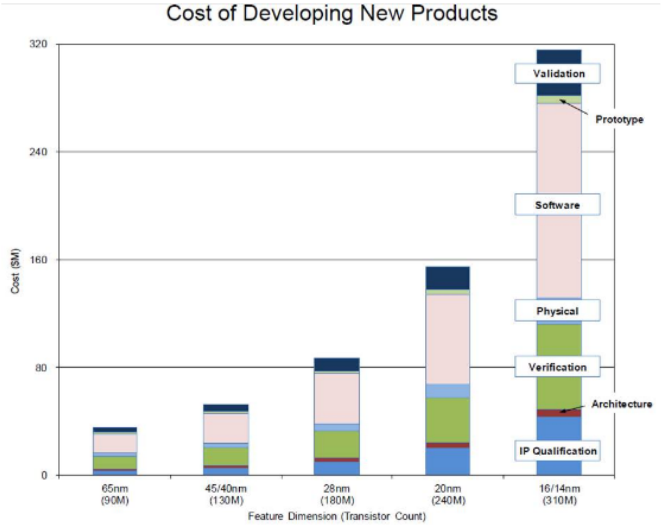
Source: Bloomberg, BofA Merrill Lynch Global Research Estimates

Figure 7: Dramatic Rise in Fab (left) and Design (right) Costs

5.2 Importance Of IP At Advance Nodes

While much greater functionality is possible at advanced nodes, increasingly complex IP is necessary in order to realize it in any given product design. For example, product capability, such as processing power enabled by high density transistors in advanced nodes, can be leveraged only with sufficient bandwidth of data on and off the chip. Satisfying such requirements requires specialized advanced high-performance Input Output (I/O) circuits[12].

Figure 8: Cost of Developing Semiconductors at Advanced Nodes outlines the exponentially increasing IP costs at advanced nodes. Advanced IP generation and use is characterized by longer lead times, higher cost than prior generations, and higher risk due to the specialized skills and technology expertise required to successfully implement. Re-creating existing advanced IP is not a viable approach for the U.S. Government programs, due to high costs and lead times involved, and most importantly the lack of available fully cleared skilled critical resources available in the market for required specialties.



Source: IBS

Figure 8: Cost of Developing Semiconductors at Advanced Nodes

Consequently, advanced node use for USG programs MUST include access to leading edge commercial IP, with application of suitable vetting and reliable countermeasures at the chip and/or system integration level to address potential vulnerabilities associated with such IP being developed in non-trusted manners. The DARPA Common Heterogeneous Integration and IP Reuse Strategies (CHIPS) program[13] seeks to address some of these challenges and is a step in the right direction.

5.3 USG Misalignment With Commercial

Microelectronics have been a significant enabler of most USG systems for decades. Today, the increasing costs and globalization of the semiconductor industry preclude the USG from fully satisfying its microelectronics needs without relying on foreign commercial sources. Not only does the USG need to maintain access to a range of microelectronics, but it needs to trust the authenticity and integrity of its suppliers. The U.S. Defense Industrial base already experiences significant challenges in obtaining trusted older (a.k.a. legacy) microelectronics and these challenges cannot be allowed to afflict state of the practice or state of the art technologies.[14] The USG should maintain and cultivate positive relationships with the U.S. semiconductor industry to maximize its access to and its trust in the advanced capabilities that U.S. SOTA microelectronics can provide.

[12] http://semiengineering.com/performance-increasingly-tied-to-io/
[13] https://www.darpa.mil/program/common-heterogeneous-integration-and-ip-reuse-strategies
[14] https://www.nap.edu/catalog/23561/optimizing-the-air-force-acquisition-strategy-of-secure-and-reliable-electronic-components

A major factor that hinders USG programs from working smoothly with the commercial industry is the fundamental mismatch in USG program length of development (i.e. Major Defense Acquisition Program (MDAP)) and use cycles, performance demands, and product volumes versus commercial industry market characteristics. USG development and fielding lifecycles are typically many decades long, require significant technology maturity to meet military/aerospace (MIL/Aero) reliability and environmental needs, and demand a relatively small number of components (including replacement parts). In contrast, the commercial market typically services high volume programs and maintains production for a single decade. Furthermore, the USG is interested in developing and using systems with unique capabilities not available in the commercial market, a necessary achievement to maintain technical advantage over solutions adversaries can create with commercially available technologies. Unlike the commercial world, USG end uses are both numerous and very specific; thus few products can satisfy multiple USG end use requirements. This results in minimal opportunity to aggregating volume across USG programs

In contrast, commercial companies often adapt a smaller range of products for multiple diverse end uses to achieve high volume demand. Coupled with a financial model to amortize up front SOTA program development costs over production volumes, this approach enables an effective financing means for fabless companies to address escalating costs in newer technologies. These economics are presented in Figure 9: Effective per Unit Cost of High vs. Low Volume Programs.

Unfortunately, differences in financial treatment and USG procurement regulations preclude even modest amortization. As a result, USG program budgets must fund all up front development costs. This presents a significant barrier to USG program adoption of SOTA technologies, and hinders the ability to achieve and maintain a technological asymmetrical advantage.

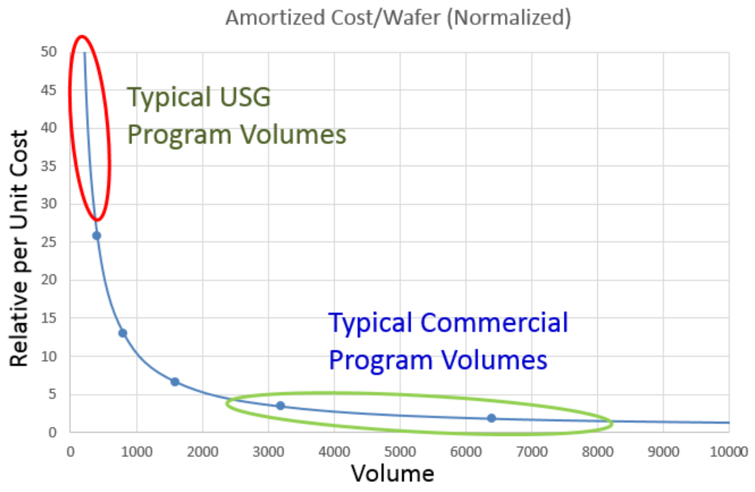


Figure 9: Effective per Unit Cost of High vs. Low Volume Programs

These differences in interests, requirements, volume demands, and fixed costs have led to USG buying behaviors that are at odds with the commercial semiconductor market offerings.

Figure 10: Contrasting USG and Commercial Operations illustrates these differences and identifies impacts to the USG's R&D and acquisition capabilities.

Commercial vs USG Program Characteristics and the Impacts on USG Systems

Up Front Development Cost (relative to total program cost)

Commercial	USG	USG Impact
Low/Med (costs amortized over volume)	High (minimal to no amortization over volume)	Higher total development cost in phases, older technologies fielded, obsolescence issues.

Production Volumes

Commercial	USG	USG Impact
Millions	Thousands	Low buying power, low market interest. Business model challenges

Total Lifecycle (development to obsolescence)

Commercial	USG	USG Impact
Development: 1.5 yrs. **Production:** 5-10 yrs.	**Development:** 10 yrs. **Fielding:** 10-25 yrs.	Rapid increase of USG systems relying upon older obsolete technologies

Amortized Per Unit Cost

Commercial	USG	USG Impact
Approaches hardware per unit cost	Dominated by Up Front Cost	Requires Significant USG program motivation to migrate to new technology nodes

Figure 10: Contrasting USG and Commercial Operations

These USG program requirements stand in stark contrast to commercial market characteristics and effectively prevent USG programs from fully accessing and leveraging commercial offerings.

Further escalating the differences, USG programs are typically procured as cost plus contracts under an Earned Value Management (EVM) approach. Progress payments are coupled to completion of individual tasks enumerated in a Work Breakdown Structure (WBS). Program funding is typically approved in phases, subject to annual USG budget constraints. The end result is a series of short-term progress payments for a subset of WBS tasks. This process does not allow USG contractors to take full advantage of commercial electronics design practices which can result in more holistic, adaptable, and cost effective outcomes. Additionally, cost-plus contracts provide little to no incentive for first-pass success. The EVM and USG annual budgeting process are a product of USG efforts to acquire multiple systems at once, rather than prioritizing the timely completion of a single new system before initiating the next one. A prioritized approach could result in better long term outcomes.

In contrast, the automotive, medical, and electronics industries, among others, have proven that sophisticated, high-quality, and profitable new products can be launched annually, and be done on a firm, fixed cost basis. The constant threat of product liability incentivized these industries to develop product development processes that "design in" quality, systems engineering, and testing.

As was cited two decades ago in a Spring 1997 article in "Acquisition Review Quarterly,"[15] adopting such commercial product development best practices would allow the USG eventually to achieve the desired goal of firm fixed price acquisition programs. Figure 11 highlights the challenges with matching the USG's desired outcome with the semiconductor market requirements.

- **USG Desired Outcome**
  - Access and Assurance of supply
  - Reduction of escalating advanced node costs
  - Obsolescence avoidance
- **Semiconductor Market Requirements**
  - Production Volume
  - Commercial Terms
  - Supplier Offering Viability
- **Multiple approaches will be necessary to simultaneously satisfy USG and commercial market requirements**

Figure 11: USG Desired Outcomes and Semiconductor Market Requirements

6 ACTIONS

6.1 Make The USG An Attractive Customer To (Needed) Commercial Partners

As a result of its low volume demand and the constraints on its procurement practices, the USG is not viewed as a particularly attractive customer to many commercial companies. Past Secretaries and Under Secretaries of Defense have appreciated this challenge and developed new acquisition mechanisms (Other Transactions Authority (OTA) and FAR Chapter 12) to make it easier for commercial companies to do business with the USG.

While the semiconductor industry was enabled by USG investment and many U.S.-based electronics companies remain committed to the national security mission, USG spending is not sufficient to constitute a primary market for these companies. To leverage their interest and investment effectively, the USG and Defense Industrial Base (DIB) should be willing to learn and to adopt

[15] http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA331994

commercial best practices, while continuing to streamline the contracting process for BOTH commercial and DIB companies.

6.2 Aggregation Solutions

As identified earlier, high fixed costs and the accompanying economies of scale both for semiconductor manufacturing and semiconductor products are making the low volume military semiconductor business economically difficult to maintain. A potential solution is to increase the total volume of manufacturing as well as increase the size of manufacturing runs. One approach is "aggregation" i.e., clustering of separate orders into a single order that can be processed in bulk.

In some ways, the pure play foundry business model already performs a level of aggregation in accepting multiple customers' production orders and processing them in a single fab to achieve high volumes of production that could not be achieved by any one program alone. Companies such as TSMC and GLOBALFOUNDRIES currently operate in this manner and achieve significant economies of scale that have literally changed the industry. Today, of the four most advanced fabs, two operate as pure play foundries each aggregating orders from many customers, while the other two remain IDMs predominately fabricating their own product streams of very high volume parts targeting their own end products that service large commercial markets (see Figure 6: Industry Consolidation).

To extend production aggregation to small markets such as the USG or even smaller, approaches such as Multi-Project Wafers and other ways of aggregating industrial product orders into a single manufacturing run could be adopted. To accomplish this effectively, the USG should establish a central order desk for all semiconductor procurements. Organizations such as MOSIS[16] and TAPO[17] already perform this function on a smaller scale and are candidates to implement this option, although potential barriers to these approaches include anti-trust concerns. Nevertheless, this could be an opportunity to reduce the cost impact to the USG of the manufacturing economies of scale and enable opportunities to be leveraged.

Additionally, NRE costs such as EDA and IP licensing continue to rise at an alarming rate, (see Figure 8: Cost of Developing Semiconductors at Advanced Nodes.) One approach to address these key costs could be to establish a design consortium to aggregate the licensing of EDA and IP for military use and focus on supporting the defense microelectronics industry. Another possibility is simply to centralize the design activity, rather than having every company in the defense microelectronics market perform its own design activity. One or more industrial centers could be created to perform SOTA design on behalf of industry and government. This model would enable aggregation of the high NRE elements of design. The outcome of a more deeply competent and resilient design capability, allowing more sharing of design/IP across industry, would be welcome. An additional

[16] Metal Oxide Semiconductor Implementation Service (http://www.mosis.com)
[17] Trusted Access Program Office (http://www.dmea.osd.mil/tapo.html)

benefit would be in identifying similar products for different customers which could be "consolidated" into a single product to meet the needs of multiple customers simultaneously.

6.3 Expanding the Market

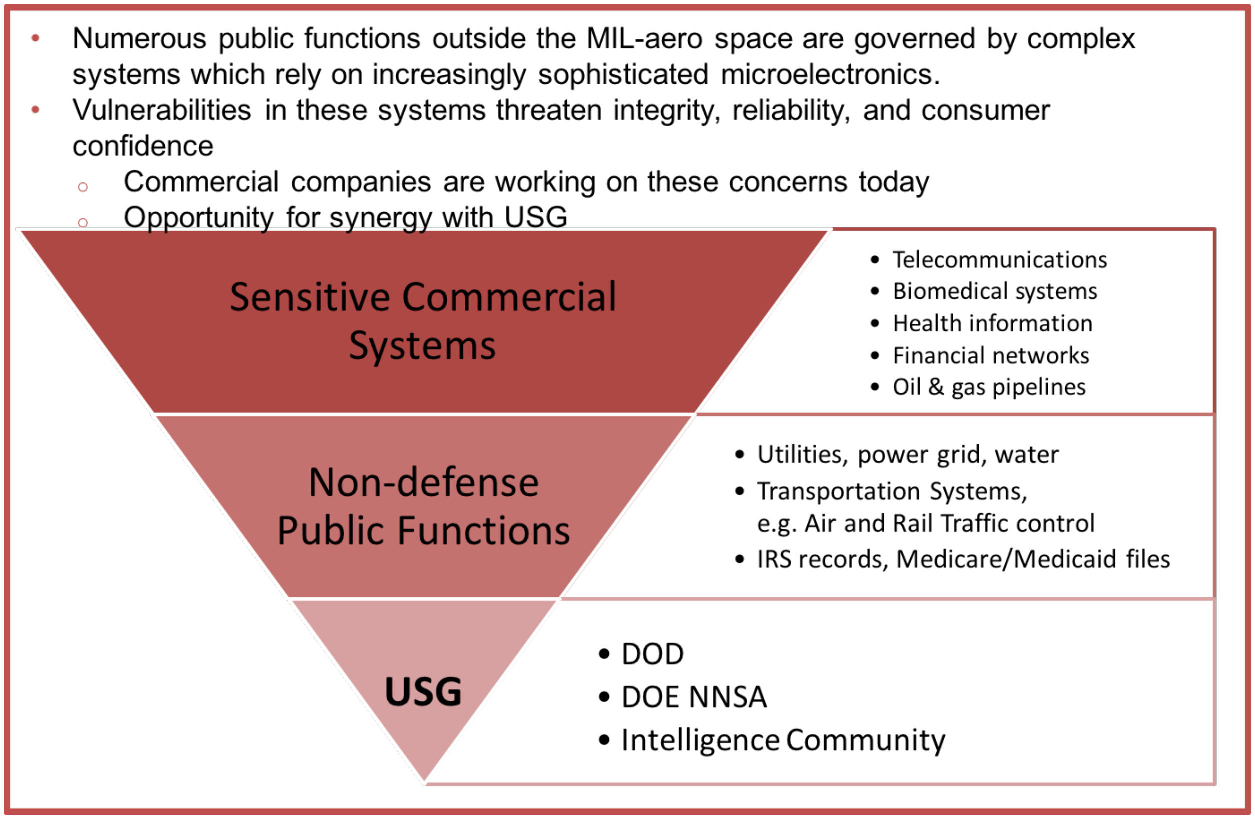
Outside of the USG, other public-sector entities and several critical industries are increasingly reliant on microelectronics systems. HPC, financial, medical, transportation, utilities, Industrial Industry of Things (IIOT), and many others require "systems of systems" for their daily operations, comprising the operation of machinery, management of information, payment systems, user data and the interaction of these components. Vulnerabilities in financial systems can cost billions and vulnerabilities in health monitoring systems threaten patient safety. Failures in the microelectronics on which these systems rely on threaten their safety, reliability, and consumer confidence.

Recent cyberattacks on sensitive civilian systems illustrate the scope and severity of the threat. These attacks can take several different forms. Ransom attacks lock up a system, withholding access until a ransom is paid. Simple data theft is exposing millions of people each year to identity theft. Not only individuals' data is vulnerable; malicious code can be employed for industrial espionage and sabotage. What may have once seemed an esoteric threat has in recent years become very real with the potential for life-altering and even life-threatening consequences.

In 2013-14, attacks on just two companies, Target and Home Depot, resulted in the theft of over 100 million customers' credit card and debit card information. In another incident, criminals hacked into a hotel's electronic key system and held it for ransom. The hotel was unable to check guests in or out, or grant access to rooms until ransom was paid in Bitcoin. More recently and ominously, Britain's National Health Service (NHS) was the subject of an international ransomware attack in May 2017. Although patient data is not thought to have been compromised, health information systems at more than 40 NHS facilities were locked up such that hospital personnel could not access patient records. The result was that appointments and procedures had to be rescheduled, and prescriptions could not be filled. One can extrapolate from these examples to the financial and safety risks of comparable breaches in transportation or utilities systems.

Clearly, the need for greater security in electronic systems goes well beyond the realm of the national security community. Indeed, the defense community has a lot to gain by reaching out to civilian government agencies and these industries, both to share information and to drive requirements. Together, the combined demand for trusted microelectronics from a broader coalition can mitigate what has heretofore been a seemingly intractable tension between the costs of "trusted" microelectronics and the very small volumes of the boutique defense market.

This broader interest in improving the security of microelectronics systems represents an opportunity to address the challenges of the USG's very small volumes. The USG could encourage or even require the use of secure components in selected commercial applications, perhaps with varying tiers of security depending on the level of risk. At a minimum, the use of trusted or secure elements throughout private sector systems should be encouraged as an industry “best practice.” The “Energy Star” label could be a model for an incentives-based approach. As the preceding examples show and as depicted in Figure 12: Opportunities for Synergy Outside USG, private industry has an enormous financial stake in security. The ability to protect data and ensure the security of critical systems can be a tremendous competitive advantage if companies see a straightforward path to define requirements and acquire more secure electronic components. The solution that would increase demand and lower costs for USG, then, requires a substantial outreach and education effort among civilian agencies and private sector stakeholders, coupled with a process for defining tiers of security commensurate with risk and promoting adoption.



- Numerous public functions outside the MIL-aero space are governed by complex systems which rely on increasingly sophisticated microelectronics.
- Vulnerabilities in these systems threaten integrity, reliability, and consumer confidence
  - Commercial companies are working on these concerns today
  - Opportunity for synergy with USG

Sensitive Commercial Systems

- Telecommunications
- Biomedical systems
- Health information
- Financial networks
- Oil & gas pipelines

Non-defense Public Functions

- Utilities, power grid, water
- Transportation Systems, e.g. Air and Rail Traffic control
- IRS records, Medicare/Medicaid files

USG

- DOD
- DOE NNSA
- Intelligence Community

Figure 12: Opportunities for Synergy Outside USG

6.4 Trust Model Evolution

Currently there is no semiconductor company that is fully Trusted accredited for SOTA technologies. As a result, the USG and U.S. DIB are in essence precluded from using SOTA technologies. This problem is rooted in DODI 5200.44, which requires that Application-Specific Integrated Circuits (ASIC)” be procured from a trusted accredited supplier (using trusted processes). This necessarily limits which suppliers can be utilized by the U.S. DIB.

Programs under 5200.44 programs may deviate from trust requirements only by obtaining a waiver to accept risk mitigation schemas documented in a Program Protection Plan (PPP)[18,19]. In absence of trusted supply at each supply chain element of the E2E Flow, creating acceptable security constructs is extremely challenging. It requires enormous effort from all parties involved (including from suppliers), is neither scalable nor timely, nor is rarely approved.

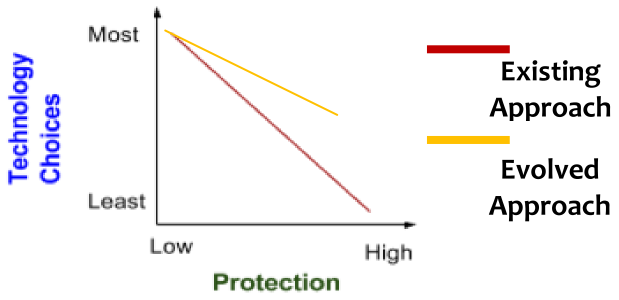


Figure 13: Impact of Potential Trust Model Evolution

This process requirement presents a technology choice dilemma to programs, as depicted in Figure 13: Impact of Potential Trust Model Evolution. The greatest number of technology choices exist for purely commercial supplier offerings, whereas the least number of technology choices exist for the subset of suppliers that are trusted accredited. The most advanced technologies (below the 32nm node) are not available as trusted, and only one pure play foundry supplier exists in the U.S. for such SOTA technologies. Programs subject to DoDI 5200.44 are challenged to determine a compliant solution and are presently prohibited from utilizing non-Trusted sources and therefore face limited availability.

A significant opportunity exists to increase the *availability* of a non-trusted E2E supplier offering services to USG and U.S DIB programs, while simultaneously addressing the *confidentiality* and *integrity* requirements of the USG. The requisite information (Supply Chain Risk Management (SCRM) program requirements, vulnerabilities and countermeasures, independent security assessments, etc.) exists within different entities of the DIB. A comprehensive tool could be developed to reconcile the wide range of considerations to accomplish efficient program level risk assessments, modify PPP's and inform related security approval decisions. With this approach, security at each element of the E2E Flow could be efficiently reconciled, assessed and evaluated on a per product basis, with increased *availability* of commercial element offerings to USG programs as a result. Having such an efficient and agreed upon approach would immediately increase *availability* of advanced technologies to USG programs. The following factors, including Figure 14: Attack Countermeasure Opportunity, should be

- **Evaluation of attacks across ASIC development lifecycle help identify areas of particular vulnerability**
- **Countermeasures, trust, or both, can improve assurance of devices**

Figure 14: Attack Countermeasure Opportunity

[18] http://www.acq.osd.mil/se/docs/PPP-Outline-and-Guidance-v1-July2011.pdf

[19] https://www.dau.mil/tools/dag/Pages/DAG-Page-Viewer.aspx?source=https://www.dau.mil/guidebooks/Shared%20Documents%20HTML/Chapter%209%20Program%20Protection.aspx

considered in development of this evolved approach:

6.4.1 Supplier Vulnerability Assessment Catalog (SVAC)

Vulnerability assessments across each E2E Flow element, from all suppliers the USG and U.S. DIB can access commercially (trusted accredited or not) could provide a basis of risk assessment for possible attacks of importance at each step in the E2E flow. See the next section, E2E WORKFLOW VULNERABILITY ASSESSMENT, for further details.

6.4.2 Countermeasure Techniques

DARPA and parties within the U.S DIB are developing security countermeasure techniques that can be applied during design, test, verification, or other stages of the E2E Flow (i.e. supply chain). Once demonstrated, these may provide viable means of adequately mitigating certain *confidentiality* and *integrity* concerns when sourcing portions of the E2E Flow from non-trusted accredited suppliers. Such countermeasures can reduce the probability and/or impact of attacks, and must be factored into a net assessment of risks from the SVAC for selected elements of supply in the E2E flow.

6.4.3 End Use Confidentiality and Integrity Requirements

End-use requirements can drive differentiating sensitivities to *confidentiality* and *integrity* concerns (on a per program basis). For example, communication gear to be worn by a soldier may be produced in high volume, and due to the nature of warfare, such units will inevitably fall into enemy hands. Thus, *confidentiality* risks must be addressed robustly. One *confidentiality* mitigating approach is for each end use unit to include anti-tamper response means (at the system level). Since these system level countermeasures must be implemented for the targeted end use, such mitigation could justify sourcing certain elements of the E2E Flow from sources that may not be Trusted accredited, but with assurances that *integrity* concerns are still addressed. Other end uses, such as for satellites, may have a lower risk of acquisition by an adversary, and may not require the same countermeasures at the system level, but instead require trusted accredited sources for all elements of the E2E Flow. Such differentiating risk sensitivities must be factored into the criteria that a given program must satisfy at each element of the E2E Flow.

6.4.4 Satisfying DODI 5200.44 Trust Requirements

DODI 5200.44 states

> e. *In applicable systems, integrated circuit-related products and services shall be procured from a trusted supplier using trusted processes accredited by the Defense Microelectronics Activity (DMEA) when they are custom-designed, custom-manufactured, or tailored for a specific USG military end use (generally referred to as ASIC.*

The present wording implies that a single supplier, with *Trusted* accreditation, would provide each element of the E2E Flow to create a microelectronics device, whereas in reality programs must select from multiple suppliers (especially for SOTA) to piece together a supply chain solution for each program. If this evolved approach — providing comprehensive trust and security by combining a range of different trust enhancement and hardware vulnerability countermeasure techniques — does so by utilizing different sources, could DODI 5200.44 be satisfied? If not, changes to DODI 5200.44 may be required to adopt the programmatic application of countermeasures and program requirement variability being proposed here.

6.5 E2E Workflow Vulnerability Assessment

To increase *availability* of microelectronics, in support of trust model evolution, a quantitative analysis of risks encompassing not only attack vectors at each step in the E2E Flow, but also possible countermeasures, can define a trade space for each program to find appropriate E2E Flow supplier elements (that reconcile countermeasures) and meet end use requirements. To be relevant, the model must be practical, easy to use, and efficient, built upon a framework of causal risk assessments and countermeasures that are determined by an independent body (TAPO is well positioned to fulfill this role today.)

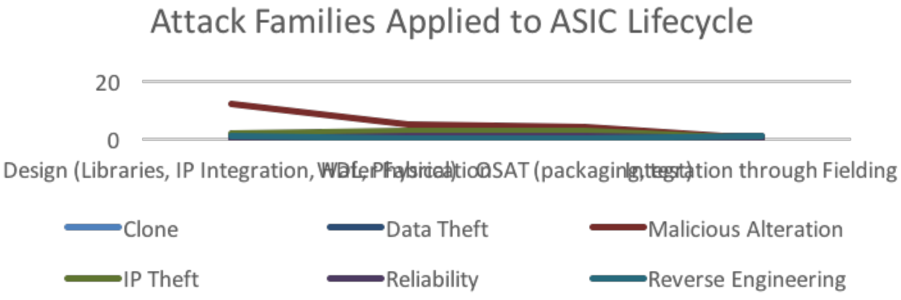


Figure 15: Representative Attack Analysis

A representative Attack analysis is shown in Figure 15: Representative Attack Analysis. This figure depicts typical relative risk magnitudes across E2E Flow elements, for several attack categories such as Malicious Alterations and Reliability (*integrity* concerns), Cloning and IP/Data theft and Reverse Engineering (*confidentiality* concerns). Focusing on Malicious Alterations for example, we can observe that relative risk is highest early in the E2E Flow. Such a risk profile must be understood and addressed to provide appropriate protections such that Malicious content is not inserted by potential bad actors in the Design phase. Carrying this forward in the E2E Flow, relative risk for malicious content insertion is significantly lower through the wafer fabrication step, and therefore the level of protection measures required during wafer fabrication may not be as comprehensive as during the design phase.

To apply this technique in a programmatic manner for assessing trade off decisions between Risks and Costs and *availability*, analysis is then required to look at resulting *integrity* at each step of the E2E Flow. In this example shown in Figure 16: Representative E2E Flow integrity Analysis, we continue examining a representative program with a sourcing option trade space of (1) Commercial, (2) Commercial with Countermeasures, (3) Trusted accredited, and (4) Trusted accredited with Countermeasures.

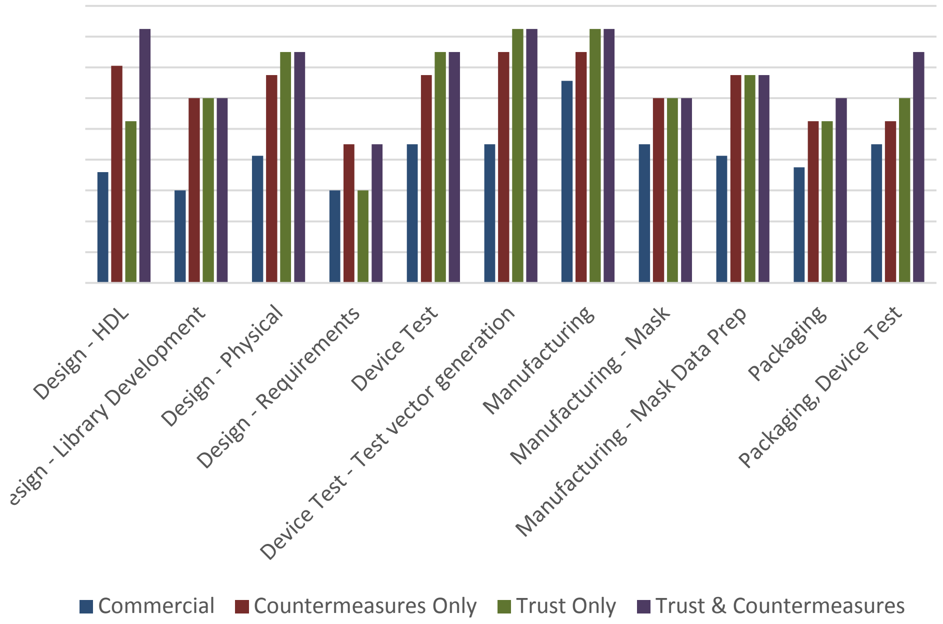


Figure 16: Representative E2E Flow integrity Analysis

We can observe that comparing *integrity* during the High-Level Design (HDL) step to the *integrity* during fab/Manufacturing, that one must apply Countermeasures or Trust and Countermeasures, to achieve the same level of *integrity* as achieved with just the Commercial sourcing for fab/Manufacturing. For a given technology, only a subset of this option space will be available from suppliers, and as observed earlier, no trusted accredited fab manufacturing is available for SOTA technologies. Following this example through, one could possibly apply countermeasures to enable selection of a commercial only fab for that element in the E2E Flow, while selecting Trust or Trust and Countermeasures for other available E2E Flow elements, and still achieve a high level of *integrity* in the resulting Microelectronics device.

Standardizing this process into an Analytic Framework can provide a means to determine efficiently how much assurance can be achieved for a given program. Such a process will help the program examine a range of different countermeasure combinations. For example, it may be necessary to decide whether countermeasures alone are sufficient when the trust ecosystem is not available for a specific technology, or if certain trusted accredited elements are required and must be added to a target technology through selective Government-Industry partnerships with Government investment. Exemplary processes and tools surrounding this Analytical Framework are being developed by a subset of this NDIA team to demonstrate a potential approach to arriving efficiently at the optimal program level decisions for desired end system assurance goals.

6.6 Call For National Semiconductor Strategy

The United States must maintain its global leadership in the semiconductor industry for both national security and economic vitality. As Defense Secretary Carter stated in 2016, "our reliance on technology has given us great strengths and great opportunities, but also led to vulnerabilities that adversaries are eager to exploit."[20] On a more relevant note, Marine Corps Vincent R. Stewart, Defense Intelligence Agency Director on June 7, 2017, referring to the IC's failure to embrace a digitial future stated: "The Intelligence Community I believe is facing its own Kodak moment, right now, all around us. If we don't address it, we will be left behind, our stock will be worth less than Kodak."

The United States must not allow its leadership in this fundamental technology area to be lost. In addition to their fundamental significance for the Department of Defense as a supplier of essential components for critical systems, semiconductors were the fourth ranked U.S. export product in 2016, behind aircraft, refined oil, and automobiles. An effective national strategy would encompass a number of different policy mechanisms, including – but not limited to – domestic R&D investment, tax and trade policies, IP protection, high skilled immigration reform and measures to ensure access for critical government functions, such as national defense. Multiple studies conducted in recent years detail the key components of a comprehensive national strategy.

The U.S. semiconductor industry is most successful outside the manufacturing domain, i.e., research, design, materials, packaging, test. Although the U.S. has the world's most advanced technical base, manufacturing capacity growth outside the U.S. has been enabled by conscious public sector strategies, whereby other countries are investing billions of dollars in building native semiconductor manufacturing capabilities.

Countries such as China, Taiwan, and South Korea are funding its development and taking steps in policy to support industry growth. For example, China has published a national plan, in partnership with regions and localities, to cultivate and expand its domestic capabilities in the semiconductor industry. This plan includes detailed goals, such as increasing domestic production to meet 70% of its domestic demand by 2025. According to their 13th five-year plan, China explicitly seeks to develop an entire semiconductor industry that includes logic, memory, analog, FPGA, power management ICs, semiconductor manufacturing equipment, CAD, and EDA tools. According to IC Insights, China's memory needs (DRAM, NAND Flash, NOR and other memories) account for 25-27% of domestic IC purchases. To achieve its goals, China has promised to invest up to $150 Billion over the next ten years. It has already taken steps towards these goals, pledging $70 Billion for building advanced memory fabrication facilities in 2017/18 alone. Action to establish a U.S. National Semiconductor Strategy is urgently required.

[20] DoD Secretary Ashton Carter, D*efenseone.com/technology, "Carter May Elevate Cybercom to a Full Combatant Command", April 5, 2016*

6.7 The Need For Public-Private Partnerships

In November of 2016, PCAST launched a semiconductor working group to examine ways to strengthen U.S. leadership in the semiconductor industry in the face of increasing globalization, consolidation, and aggressive actions by other countries. The recommendations of the PCAST working group focused primarily on macroeconomic policy measures such as trade, tax, and IP protections, as well as recommendations for bold, targeted R&D programs, like that of the cancer moonshot[121]. In this paper, we endorse the high-level recommendations of the PCAST working group, in regard to the trade, tax, and IP protections. Drawing on the expertise of the working group, we further recommend public-private R&D partnerships to support manufacturing, IP development, EDA tool development, and workforce training. These partnerships should include but extend well beyond the USG, to the broader community of interest in hardware security. Such R&D partnerships should provide shared facilities, prototyping, testing and evaluation services for the development of critical technologies for new hardware security capabilities, as well as low-volume, high-mix production of leading edge and emerging technologies. Taking a broader view in supporting hardware security R&D, well beyond the national security community, will maximize the ability of such partnerships to engage with the commercial semiconductor industry, build sustainable operating models for the long-term, and serve the widest range of public interests.

Microelectronic systems undergird U.S. critical national infrastructure for both public and commercial functions.

7 SUMMARY

Over the past 70 years, the microelectronics industry has evolved from a boutique industry to become a complex, global, and dynamic industry driven by commercial market forces. Today, microelectronics components and systems underpin the business processes and consumer activities of nearly every sector of the global economy. Government purchases, particularly the specialized purchases for defense systems, account for a small fraction of the whole. A significant proportion of manufacturing has moved off-shore where Asia-Pacific leads with two thirds of worldwide capacity. Nonetheless, the USG still requires access to leading edge microelectronics technologies that are both trusted and cost effective for secure communications, superior weapons systems, and other sensitive functions.

A strong domestic industry is vitally important for the U.S. economy as a whole, and better alignment between USG and commercial business models are essential to assure USG access to SOTA technologies. A coordinated strategy can be –and has been– very effective for focusing scarce

[21] https://obamawhitehouse.archives.gov/the-press-office/2016/02/01/fact-sheet-investing-national-cancer-moonshot

resources where they will have the greatest impact. Such a strategy should include *investments* in R&D infrastructure, *reform* of acquisition and other "business" practices, and *expansion* of the market for hardware security.

Invest: The Infrastructure of Innovation

Shared infrastructure to support pre-competitive R&D and to build manufacturing capability is a critical element of an ecosystem that fosters innovation and encourages new entrants to the industry. Targeted measures to support this goal could include:

- Increasing USG investment in semiconductor R&D
- Improving access to IP: Create a central "Trusted IP" database and IP accreditation process
- Improving design capabilities: Establish a Center of Excellence for design
- Developing manufacturing capabilities: Establish public-private partnerships or consortia to address challenges such as novel materials integration, EDA tool development, and workforce training. Develop a prototyping resource for the USG, the DIB, the national and services labs and FFRDCs.

Reform: USG acquisition alignment with commercial

USG acquisition operations do not align with commercial market business models in terms of volumes, lifecycle lengths, technical requirements, and contracting terms, among other things. Furthermore, USG purchase volumes are too small to influence commercial industry, so better alignment with market practices is critical to maintaining access. Recognizing and capitalizing on the growing need for more robust security in commercial systems could result in aligning USG and commercial demands for robust onshore industry. Productive measures would include:

- Centralizing acquisition with aggregated USG demand (possibly by expanding TAPO's role?)
- Embracing an End-to-End trust perspective, including countermeasures, in order to leverage SCRM
- Testing new contracting mechanisms, training USG acquisition and Program Management workforce and incentivizing contracting officers to use streamlined mechanisms
- Highlighting the necessity of using the most advanced technologies to maintain technological superiority

Expand: Drive adjacent complementary commercial market demand in the U.S.

The USG is not the only entity that has a material interest in hardware security. Indeed, latent demand for secure microelectronics is high among public and private sector entities. This untapped market represents an opportunity for both the commercial industry and for the USG to increase availability and reduce the cost of secure microelectronics supply. Relatively simple measures, including education and outreach, can yield a disproportionately significant benefit to both parties:

- Trust framework expansion: Establish levels to fit a broad range of needs and capabilities, as well as to encompass more technologies (ASICS, FPGAs, COTS/GOTS/MOTS, etc.)
- Develop dual-use technologies with security enhancing possibilities such as component tracking, advanced packaging, non-silicon tech integration, among others
- Facilitate targeted outreach to raise awareness and increase demand for more secure systems in commercial markets

These targeted measures, coupled with a broadly supportive economic policy environment, can facilitate a win-win outcome: increased demand for secure microelectronics, better access for the USG, new tools to better defend against cyber supply chain attacks, and more security for critical infrastructure and sensitive commercial systems.