

**Spring 2018
Industry Study**

**Industry Report
*Electronics***

13

REVIEWED BY DOD

DEFENSE OFFICE OF PREPUBLICATION AND OFFICE OF SECURITY REVIEW

NO CLASSIFIED INFORMATION FOUND

Mar 20, 2019



**The Dwight D. Eisenhower School for National Security and Resource Strategy
National Defense University
Fort McNair, Washington D.C. 20319-5062**

ELECTRONICS 2018

ABSTRACT: The electronics industry is a group of firms involved in one or more aspects of the design, manufacture, testing, assembly, and packaging of microelectronic semiconductor integrated circuits (ICs). As a whole, the global electronics industry is healthy, having benefited from tremendous market growth made possible by Moore’s Law, disaggregation in some market segments, and consolidation in others. ICs are critical components of U.S. government capabilities related to national security, and currently these devices have no substitute. Given the strategic importance of microelectronic semiconductors in U.S. national security systems, the weak market position of the U.S. government as a buyer, and the industry’s global process disaggregation and dispersion trends, the U.S. government must actively manage assured availability and trusted access as well as supply chain risks and vulnerabilities while increasing investment in basic research, enhancing incentives for innovation and development, and preventing the transfer of critical technologies and know-how to potential adversaries.

LTC Michelle Bronell, U.S. Army
COL Vepkhvia Chalabashvili, Georgian Army
COL Claudio De Oliveira, Brazilian Air Force
LTC Anthony Gibbs, U.S. Army
LtCol David Manka, U.S. Marine Corps
Lt Col Christopher Meeker, U.S. Air Force
COL James Nelson, U.S. Army
Lt Col Victoria Nemmers, U.S. Air Force
Lt Col Ryan Novotny, U.S. Air Force
Mr. Alan Philpott, U.S. Department of Navy
Captain Ferdinand Reid, U.S. Navy
Mr. Tod Reinert, U.S. Department of Homeland Security
Dr. Judd Stitzel, U.S. Department of State
Lt Col Joshua Williams, U.S. Air Force

Dr. Peter Coughlin, Faculty Lead
Mr. Robert Bestani, Faculty
Mr. Andrew Wylegala, Faculty

Industry Study Outreach and Field Studies

On Campus Presenters:

Boeing
 Electronic System Design Alliance (formerly Electronic Design Automation Consortium)
 IBM
 Office of the Deputy Assistant Secretary of Defense Manufacturing and Industrial Base Policy
 Institute of Defense Analyses
 Rochester Electronics, LLC
 Naval Research Laboratory
 BAE Systems

Field Studies - Domestic:

Semiconductor Industry Association (SIA), Washington, DC
 Defense Advanced Research Projects Agency (DARPA), Arlington, VA
 Micron Technology, Manassas, VA
 Northrop Grumman, Linthicum, MD
 ACDI, Nashville, NC
 Wolfspeed, Durham, NC
 North Carolina State University, Raleigh, NC
 - PowerAmerica
 - Center for Additive Manufacturing and Logistics (CAMAL)
 - The Nonwovens Institute (NWI)
 - Future Renewable Electric Energy Delivery and Management Center (FREEDM)
 eSilicon, San Jose, CA
 Electronic System Design Alliance (ESDA), Mountain View, CA
 Mentor Graphics, a Siemens Business, Fremont, CA
 Semiconductor Equipment and Materials International (SEMI), San Jose, CA
 ARM, San Jose, CA
 Computer History Museum, Mountain View, CA
 NEXTFLEX, San Jose, CA
 U.S-Asia Technology Management Center, Stanford University, Stanford, CA
 SRI International, Menlo Park, CA
 ASML, San Jose, CA
 Advanced Micro Devices (AMD), Santa Clara, CA
 Intel Corporation, Santa Clara, CA
 ESD Alliance CEO Outlook, San Jose, CA
 L-3 Corp, Anaheim, CA
 Aerospace Corporation, El Segundo, CA

Field Studies International:

Realtek Semiconductor Co., Hsinchu, Taiwan
 Taiwan Semiconductor Manufacturing Co. (TSMC), Hsinchu, Taiwan
 Etron Technology Inc., Hsinchu, Taiwan
 MediaTek, Hsinchu, Taiwan
 Industrial Technology Research Institute (ITRI), Hsinchu, Taiwan
 American Institute of Taiwan, Taipei, Taiwan
 Acer Inc., Taipei, Taiwan
 Micron, Taipei, Taiwan

INTRODUCTION

The electronics industry, for the purpose of this study, is defined as the group of firms that engage in one or more aspects of the design, manufacture, testing, assembly, and packaging of microelectronic semiconductor integrated circuits (ICs). As a whole, the U.S. electronics industry is healthy. Many old and new firms have flourished thanks to Moore's Law and market growth, despite industrial disaggregation consolidation and high entry barriers, particularly in manufacturing. Industry revenues have tripled over the past 20 years,¹ and new semiconductor applications (e.g. cognitive computing, artificial intelligence) combined with growing markets in Asia portend an additional 50% growth over the next five years.²

ICs are critical components to U.S. government national security capabilities and are prolific in space, nuclear, intelligence, missile defense, land/air/sea platforms, and command and control applications. While the industry is healthy, the U.S. government faces several challenges to resource the required ICs. These include:

- Commercial market forces drive the electronics industry, and the center of gravity is increasingly shifting to Asia and especially China. ICs are in almost every military system, but the U.S. military demand represents only 0.3% of the industry.³ DoD has unique performance requirements and little market power to influence industry structure, conduct, or performance, making DoD susceptible to access, availability (i.e., obsolescence), and supply chain security risks. The same is true of other U.S. national security organizations.
- Electronics industry supply chains are increasingly disaggregated and geographically dispersed. From design to packaging, a typical IC undergoes production processes in more than four countries on several continents and travels more than 25,000 miles.⁴ This highly global and interdependent supply chain is increasingly vulnerable to disruption (access) and malicious activities (assurance).
- Risks to the U.S. government include counterfeit parts, intellectual property (IP) theft, and malicious tampering, which may cause premature failure or introduce cyber or espionage vulnerabilities. Market forces do not create industry incentives to address these requirements, and burgeoning device complexity precludes the U.S. government's ability to inspect/test for these vulnerabilities.

Given the strategic importance of microelectronic semiconductors in providing leading edge performance for national security and defense systems, the U.S. government—in its roles as sponsor, buyer, and regulator—must actively manage risks associated with access, availability, and supply chain vulnerabilities, while fostering an environment in which the U.S. industry can flourish, meet national security needs, and retain its technological edge and global competitiveness. Government efforts should concentrate on (1) fostering future U.S. IP development, (2) balancing supply chain risks of access and security assurance, (3) reducing availability (obsolescence) risks, and (4) preventing the transfer of critical technologies and know-how to potential adversaries.

ELECTRONICS INDUSTRY

The electronics industry designs, manufactures, tests, assembles, and packages ICs for electronic device original equipment manufacturers (OEMs) and other industries that use ICs in their end-products, such as the automotive, space, and defense industries. Consumer electronics comprises the vast majority of market demand, with over 86% of ICs going to communications, computer, automotive, and other consumer electronics OEMs.⁵ Asian markets account for 71% of this demand.⁶ The leading semiconductor product segments and their relative market shares are: logic devices (27%), memory devices (23%), microprocessors (18%), and analog devices (13%).⁷

The U.S. government has requirements across the spectrum of these product segments, and, a single IC may perform several applications.

The IC production process can be divided into three phases:⁸

- (1) Design: includes the transistor logic design for the specific IC function, the physical layout of the circuit on the chip, and verification of the design.
- (2) Front-end fabrication: includes the physical creation of microscopic circuits on semiconductor wafers. This phase is typically performed in highly automated, capital-intensive fabrication facilities (fabs) and requires 6-8 weeks.⁹
- (3) Back-end testing, assembly, and packaging: includes slicing the wafers into individual chips, encasing in plastic, testing, and quality control.

Once completed, the ICs are sold to electronic product OEMs for installation on circuit boards. Whether a logic, memory, microprocessor, or analog device, computational power is roughly proportional to the number of transistors in the IC. IC design is trending toward smaller, more densely populated chips with lower power consumption, higher computational speed, and higher data bandwidth to process the growing number application demands. To date, cutting-edge product lifecycles follow Moore's Law, whereby the number of transistors per square inch on an IC doubles every 18-24 months while the cost per square inch of an IC remains more or less constant.¹⁰ However, the IC industry also has followed Moore's second law (also called Rock's law, after Arthur Rock), whereby the capital cost of a semiconductor fab doubles approximately every four years.¹¹ Despite these countervailing trends, cost per transistor (which approximately correlates to computing power) has experienced a sharply downward trend.

Industry Characteristics:

The microelectronic semiconductor industry is a mature industry, characterized by significant market incentive to constantly innovate both IC devices and manufacturing processes. State-of-the-art on-chip transistor gate sizes under 10 nanometers produced on 300mm semiconductor crystal wafers is the result of continual innovation and competition. The industry is further characterized by a requirement for a high degree of manufacturing skill and significant up-front capital investment in automated fabs. Cost-effective production demands continuous, large-scale, high-volume, high-yield output to afford staggering initial fixed costs of approximately \$20 billion for a state-of-the-art fab¹² and IC design non-recurring costs approaching \$400 million.¹³ A state-of-the-art fab must produce between 30-60 thousand 300mm wafers per month to remain profitable.¹⁴ This production model presents significant barriers to entry, at least for the front-end fabrication process. In 2017 annual worldwide production capacity was 218

million wafers, and this capacity is projected to grow at an annual rate of 6% over the next five years.¹⁵ This capacity is nearly 1500 times that required to meet DoD annual IC needs.

To remain competitive in the industry, firms must continually invest a significant portion of revenues in research, development, and new capital equipment. Industry-wide investment rates average 30% of revenues over the past 20 years.¹⁶ In 2016 U.S. firms invested 18.5% of revenues in R&D alone, second only to the U.S. pharmaceutical industry investment during the same period.¹⁷

The global industry supply chain is highly dispersed. While U.S. firms command nearly 50% of the worldwide market share¹⁸ and the majority of IC design is conducted domestically, over 87% of front-end fabrication is performed outside the United States.¹⁹ Some 71% of fabrication is conducted in Asia, specifically Taiwan, South Korea, Japan, and China.²⁰ Additionally, labor intensive back-end testing, assembly, and packaging is also performed in Asia, where labor costs tend to be relatively low.²¹

CURRENT INDUSTRY CONDITION

Industry Health:

The U.S. electronics industry is strong. In 2017 the United States led the world with 48% of the global market share and has consistently held approximately 50% share for 20 years.²² Semiconductors are America's fourth largest export by dollar value, after aircraft, refined petroleum, and automobiles. In addition, the industry is the top contributor to labor productivity growth.²³ The vast majority of front-end fabrication occurs outside the United States, but America is home to 17 fabs capable of industry standard 300mm wafer fabrication.²⁴ Additionally, the Defense Microelectronics Activity (DMEA) has accredited 75 U.S. suppliers and 19 U.S. fabs under the Trusted Foundry Program for DoD semiconductor production.²⁵

Global Market:

In 2017 total global semiconductor sales registered more than 20% annual growth as revenues topped \$400 billion for the first time in history.²⁶ In 2001 Asian markets emerged as the primary component market and accounted for more than 61% of semiconductor sales in 2016.²⁷ Firms also experienced explosive cost increases in design and fabrication due to the rising level of product complexity.

At the most modern feature sizes, few firms can afford capital expenditures exceeding \$400 million for design and \$20 billion to construct fabrication facilities.²⁸ These cost barriers drive aggressive globalization of the semiconductor value chain. The industry now consists of a mixture of a very small number of vertically integrated device manufacturers (e.g. Intel) and firms that specialize in one or two submarkets, such as design (e.g. AMD) or manufacturing (so-called pure-play foundries like TSMC).²⁹

As of 2017 89% of the industry capacity of 2.3 million wafers per month resides in the Asia Pacific region.³⁰ Direct investment from national government sources manipulates the industry high capital cost barriers to entry. China and Saudi Arabia plan to expend \$150 billion and \$100 billion, respectively, to further develop their production capacity.³¹ Likewise, the 2015 sale of IBM's trusted foundry operations to the United Arab Emirates-backed Global Foundries provides an example of market activity that threatens the U.S. vertically integrated ecosystem supporting national security.³²

Five-Forces Analysis:

Harvard Business School Professor Michael Porter's five forces model is a popular, nearly four-decade-old industry analytic tool. Porter's framework evaluates competitiveness and profitability of firms through a cumulative assessment of the threat of new entrants, threat of substitutes, bargaining power of suppliers, bargaining power of buyers, and rivalry between firms.³³ The following analysis includes the commercial and military specific front-end semiconductor production in aggregate.

Threat of New Entrants: In terms of pure market forces, high capital costs and reliance on economies of scale make the threat of new entrants to the semiconductor market low. While some firms disaggregate design and manufacturing processes, costs in each of these functional areas continue to grow as circuit complexity increases. Combined capital, research and development expenditures average 30% of industry sales,³⁴ with U.S. firms investing \$56.9 billion in 2016.³⁵ As national governments increasingly engage in direct investment or subsidizing activity, the firm's barriers decrease, while simultaneously increasing for prospective competing firms. Successful return on fixed cost investments requires large production runs to develop profitable economies of scale. For U.S. government business, new entrants face the burdensome bureaucratic process of gaining accreditation as a trusted foundry.³⁶ Once approved, a DMEA-certified design or fab activity incurs oversight burdens beyond the complexity required for commercial market competition.

Threat of Substitutes: Few, if any, alternatives can fully substitute the function of semiconductors for consumers. Since chips are embedded at the core of higher integrated systems, substitution may result in the rejection of an electronic-enabled feature in final products. For example, the automobile industry offers buyers enhanced safety options, entertainment systems, and the future potential of driverless vehicles. A driver that does not select these options assumes risk, reduces feature cost, and forgoes automation for human control. U.S. government consumers face similar trade-offs in the pursuit of weapon system superiority. Navigation with a compass is cheap, but national defense and security agencies value the multiple operational advantages of precision GPS receivers. As the government and commercial markets seek to maintain consistent technical and performance advantages over competitors, the threat of substitution is low.

Power of Suppliers: A 2016 industry report on the global value chain notes, "one U.S. semiconductor company has over 16,000 suppliers worldwide."³⁷ The complexity and cost of modern chip production drives the specialization along the value chain. Suppliers exert a moderate level of power organized toward design tools, fabrication equipment, and material inputs to the industry. Computer-aided engineering tools are required to manage modern semiconductor design operations. Chemicals, elemental gases, and metals are widely available as multi-industry inputs. Advanced photolithographic equipment suppliers exert unique power in the industry, as three firms command technology vital to achieving cyclical reduced feature sizes and capture high capital costs for retooling, with just one firm able to provide equipment to create the smallest IC feature sizes.³⁸ These forces are likely to persist because supply-side firms with highly developed skill sets have effectively organized around two global industry associations, the Electronic Systems Design Alliance and SEMI.

Power of Buyers: The global semiconductor market maintains well-developed product segmentation and a steady compound annual growth rate of 9.5%.³⁹ Buyers at the OEM or distributor level face low switching costs as they purchase bulk lower-tier components. Price

sensitivity tends to be low since microelectronic component costs usually comprise a small fraction of overall end-item and project budgets. Aviation or automobile programs, for example, are willing to accept small-scale cost trade-offs for proven electronic component performance and reliability. The U.S. government's buying power is much less than the moderate power of large commercial customers. Defense spending accounts for approximately \$5.1 billion of the over \$412B market in sales, with less than \$1.5 billion allocated for military specific devices.⁴⁰ DoD experiences reduced buying power without commercial applications due to low-volume production runs, restrictive security regulations, and the cyclical loss of commercially outdated technology nodes.

Industry Rivalry: Semiconductor firms exhibit high levels of rivalry. State ownership in foreign global firms, government-backed partnerships, and capital costs elevate exit barriers. National security concerns also motivate actors to compete beyond pure market-based drivers. U.S. maneuvering to reinforce economic security and trusted access to semiconductors is at odds with national moves in the Asia-Pacific region supporting the "Made in China 2025" policy.⁴¹ These factors create highly committed competitors.

Rivalry also organizes according to high price-based forces. Demand for consumer electronic products dictates the market for component part production. Design and capital investment for fab equipment generate high fixed costs amortized across large volume production. Low marginal cost per semiconductor chip in an established fab node incentivizes high automation, process control, and facility utilization. New fabrication nodes added to global capacity often generate large stepwise additions to market volume. Adding large increments of production can result in supply shocks from overstocked inventory.

Industry Trends:

The IC market is increasingly driven by commercial interests. Demand is moving from computing (PC and tablet) and connecting (smart phones, internet) to sensing and recognizing. Over the next five years demand is forecast to be driven by the following commercial opportunities:

1. Internet of things (IoT), including artificial intelligence (AI) and machine learning
2. Virtual reality and augmented reality products
3. Big data systems
4. Automotive electronics, including connectivity, safety, and autonomous driving features
5. Smart phones
6. PC tablets, data center servers supporting cloud computing
7. Wearable electronics, including medical, and fitness trackers

These applications will demand significant increases in memory and processing speed, with power consumption a critical constraint. As production technology reaches the physical limits of IC feature size, designers and manufacturers are overcoming the end of Moore's Law through increased use of three-dimensional architectures, new semiconductor material combinations, and heterogeneous packaging such as system-on-a-chip (SoC) and system-in-a-package (SiP) technologies.⁴² These complex ICs combine multiple semiconductor products (memory, logic, processors) onto a single chip or in tightly integrated packages to shorten interconnects, thereby increasing speed while lowering power requirements. In order to leverage the defense benefits of these commercially driven opportunities and maintain its technological edge, the U.S.

government will need access to the underlying technologies and applications but with higher security and performance.

IC device complexity (driving increasing capital/R&D costs), differing scale efficiencies across the three phases of production, and cyclical business risk are driving increasing disaggregation of production processes. Firms once established as Integrated Device Manufacturers (IDMs), which executed design, front-end fabrication, and back-end package and test, are increasingly moving toward fab-less production, where front-end fabrication is performed by “pure-play” foundries. Maximum efficiency in front-end fabrication is accomplished by producing at a consistent, high volume output, but demand for electronic end products is cyclical, driven by the business cycle. Pure-play foundries are able to reduce exposure to cyclical business risk by diversifying across a wider portfolio of IC products and for a wider variety of customers. Additionally, pure-play foundries are able to gain access to greater capital from a wider array of IC design firms in order to meet the high capital costs and build and sustain efficient production. This trend poses high risks to access, timeliness, and quality control, particularly for small customers such as the U.S. government.

Accompanying disaggregation is a trend toward geographic dispersion of the production process. Ten of the top 20 firms are headquartered in the United States, and U.S. firms command 50% of industry revenues, yet over 87% of front-end fabrication occurs offshore.⁴³ Factors influencing fab location include tax policies, environmental regulations and permitting processes, supply of workforce talent, availability and quality of water, reliability of electricity and other utilities, legal protection of intellectual property, and proximity to customers. For these reasons, growth of fab capacity over the past three years has been 2.7 times higher in Asia than in the United States.⁴⁴ For the U.S. government, this trend exacerbates supply chain security challenges.

IC complexity, requiring increasing R&D and quest for IP, combined with production efficiency that is highly dependent upon scale is driving increasing consolidation. As of December 2017, the top fifteen firms held 97% of the wafer fabrication capacity and over the past decade the number of wafer fabrication companies decreased by 20%. In the United States, the 17 fabs capable of state-of-the-art 300mm wafer fabrication are owned by only five companies.⁴⁵ Given the U.S. government’s specialized product requirements and trivial market power, this trend exacerbates challenges associated with access to production.

Regional Trends:

For the past several years Asia’s IC industry has experienced rapid development. This is especially true for Chinese firms, which enjoy strong support from the Chinese government. U.S. and Taiwanese companies remain well ahead in IC design and manufacturing innovations, as well as in total R&D investment, but China is making a concerted push to take the lead in semiconductor technology. As the world’s biggest manufacturer of mobile devices and consumer electronics, China imported \$227 billion of semiconductors in 2016, almost double its oil imports.⁴⁶ In 2014, the Chinese government created a special fund to invest in the semiconductor industry, initiating a strategy that “relies in particular on large-scale spending, including \$150 billion in public and state-influenced private funds over a 10-year period, aimed at subsidizing investment and acquisitions as well as purchasing technology.”⁴⁷ Under this

strategy, Chinese firms are expected to double their market share from 20% in 2016 to 40% by 2020, and to 70% by 2025.⁴⁸

INDUSTRY CHALLENGES

U.S. firms face a spectrum of challenges in maintaining competitive advantage and market share. These challenges include foreign government subsidies (e.g. Made in China 2025), access to talent, complex/diverse tax and trade policies, and burdensome federal policies for certifications and contracting. However, the primary U.S. government challenge is to maintain access to the electronic components required to maintain national security, guarantee that electronic components meet quality and security standards, and ensure continuous availability of electronic components throughout crises and conflicts.

Access:

The primary challenge to national security stems from a combination of industry's willingness to produce for the U.S. government's unique requirements and the potential for disruption of a fully globalized supply chain. While an abundance of capacity exists to meet national security and defense demands, firms may be unwilling to commit production because of inherent difficulties working with the U.S. government (e.g. small lot production, regulation compliance) that may disrupt their ability to remain competitive in the much larger commercial market. At the same time, supply disruption risk stems from the globalized industry creating critical system nodes in potentially geopolitically contentious regions. Fabrication capacity is well-entrenched and unlikely to move back to the United States even with aggressive policy changes. America still maintains world leadership in areas of "fabless" semiconductor work (the creative design and programming aspects of the industry) as well as fabrication automation equipment. However, those areas are also at risk of offshore migration, primarily due to lack of Science, Technology, Engineering, and Mathematics (STEM) skill sets in the U.S. workforce and increasingly restrictive migration policies.

As a result, no firm or nation currently has the capacity to serve consumer or national security demands solely using assets within its own borders. While the United States is highly reliant on Asian fabrication, Asian countries are just as reliant on U.S. IP and equipment manufacturing. This global economic interdependence may help deter major conflicts.

The risk to U.S. national security becomes manifest when layered with China's stated goals and known investments. "In June 2014, the State Council of China released the National Guidelines for Development and Promotion of the Integrated Circuit (IC) Industry...with goals to increase its self-sufficiency rate for integrated circuits to 40% by 2020 and to 70% by 2025."⁴⁹

To meet this goal, China made an estimated \$55B investment in fabrication facilities. China has made similar policy goals and financial investments in both capital-intensive intellectual and manufacturing equipment capabilities. What would happen to U.S. government supply chain and capabilities if China gains self-sufficiency and complete freedom of geopolitical action and then aggressively restricts or eliminates U.S. access to the Pacific supply chain? In that case, the U.S. government likely would not be able to perform many national security functions or engage in long-duration conflict without major mobilization of U.S.-based fabrication.

Assurance:

From design to packaging, a typical IC will undergo production processes in more than four countries on several continents and travel more than 25,000 miles. While U.S. firms command

nearly 50% of the market, only 13% of IC fabrication capacity exists in the United States and recent growth in capacity is 2.7 times higher outside America. This highly global and interdependent supply chain is increasingly vulnerable to disruption and malicious activities, posing a trust and assurance risk to the U.S. government. Specific threats include counterfeit parts, intellectual property theft, and malicious tampering (quality escape or insertions) that may introduce premature failure, cyber, or espionage vulnerabilities.

In order for the United States to retain the leading edge on technology given the unique aspects of the microelectronics ecosystem and emerging threats, there must be a better collective understanding and collaboration between government and civilian industry to address vulnerabilities without inhibiting innovation.⁵⁰ For example, the government is very concerned about the overall microelectronic supply chain and network security. On the other hand, industry is less concerned about hardware citing that security vulnerabilities are primarily introduced from the software perspective. Greater collaboration is needed to define threats, vulnerabilities, and risk mitigation strategies.

Availability:

The third challenge facing the U.S. government during a crisis or long-term conflict—in an increasingly complex and globalized economy—will be the availability of semiconductors and other electronic components required to support and sustain fielded systems installed in U.S. military aircraft, ships, submarines, land vehicles, and other weapons systems. Major drivers of the availability challenge include obsolescence, increasing demand, and the rise of globalization.

The pace of technology is driven by the commercial sector, not the U.S. government. The gap is widening between the technology in fielded U.S. government systems and the technology directly available from the commercial sector. The impact of obsolescence driven by Moore's Law is felt when electronic components fielded in U.S. government systems must be replaced due to parts failure and they are no longer available in the open commercial market.

The other major driver behind the availability challenge is increasing demand. The great technological advances in the electronics industry has led to increased demand for electronic semiconductor components for devices impacting our everyday lives such as televisions, cell phones, and cars. Today we are starting to see electronic semi-conductor devices installed in refrigerators and other "smart" appliances as a standard feature. Collectively, the growth in smart appliances and the rise of smart cars and autonomous vehicles is leading to greatly increased demand in the electronics supply chain, further marginalizing the U.S. government's market power.

This shift has created unique challenges impacting availability. Securing spare and replacement electronic components from a global supply chain can be complicated and challenging. The U.S. government has concerns not only about access and assurance but also the global supply chain's ability to meet national security and defense needs in a timely fashion. The government no longer controls the supply and support of fielded electronic systems that heavily leverage Commercial Off the Shelf (COTS) technology.

OUTLOOK

The global economy drives the demand for electronics. Emerging and expanding industrialized countries are requiring more electronics due to economic and social market forces.⁵¹ It is a time of transition in the electronics industry punctuated by new manufacturing

technologies, design changes and patterns, and greater price pressures. Over the next five years the industry expects to see more disruption than it has in the past.⁵²

The outlook includes growing opportunities for revenues, profitability, and increased customer base in the near and medium term (1-5 years). This is due to new, rapidly growing technology segments, such as AI, cognitive computing, IoT, and autonomous vehicles.⁵³ The industry also faces significant long-term (greater than 5 years) challenges as China becomes a world-class competitor and potential security threat and adapts to new flexible business models.

Demand for electronics continues to grow in communications, automobile products, wearable devices, energy production, health care, and industrial automation.⁵⁴ In order to sustain increased revenues and profits, companies will look to differentiate and diversify their products by acquiring smaller players and competitors, continuing a trend of the last five years. Not only will this increase diversification for large companies, it will also allow them to gain access to new technology and intellectual property.⁵⁵

In general, companies will continue to move manufacturing to regions where labor costs and regulations are low, where they are close to their suppliers and customers, and where tax incentives are high. With electronics end-product manufacturing continuing to move to low-cost countries, component manufacturers will have an impetus to move closer to their customers.

The Chinese government is pushing to build an indigenous, globally competitive electronics industry. In 2014 the Chinese government announced a plan to raise \$100 billion-\$150 billion in public and private funds. The goal is to be independent of foreign suppliers by being on par with the world's leading firms in the design, fabrication and packaging of chips by 2030.⁵⁶ One example of a new leading-edge technology company is Horizon Robotics, a spinoff of the Chinese Academy of Sciences. Not only has the company produced two AI processors, it was able to raise \$100 million through Intel Capital from multinational venture investors. Horizon plans to use the money to develop technologies for autonomous driving and smart cities.⁵⁷

China is also graduating millions of engineers from its universities. This has helped China grow and become an R&D center for many of the OEMs requiring semiconductors. In the past both Chinese and multinational firms focused on selling products to the domestic Chinese market emphasizing low cost over leading-edge technologies. However, as Chinese customers become more discriminating, they demand greater innovation in their electronics.⁵⁸

With IoT devices, hardware and the ecosystem must also be a strategic area of focus for securing electronic systems. "If you have social attacks, they steal your password," according to Intrinsic ID founder and CEO Pim Tuyls. "If you can hack into software, the impact scale is probably up to 1,000 users before someone fixes it. If it's the operating system, the impact is up to 10,000. But if you can fiddle with the hardware, the impact can be in the billions. Once you control the hardware you can change the software functionality and control the system."⁵⁹

With increased use of electronic systems controlled by software and firmware code, the threat of exploitation moves beyond computer systems and computer networks. It moves into communication systems, building control systems (such as heating and cooling), power generation, manufacturing security systems, autonomous transport, and smart cities. Companies must address the hardware security concern to increase consumer trust and advance IoT growth into the larger marketplace.

Firms in the electronics ecosystem must continue to adapt their models to continually evolving economic and social environments. Throughout this year's Electronics Industry Study, nearly all firms surveyed expressed frustration with current U.S. immigration policies impacting their ability to retain foreign-born university graduates from STEM fields. The shortage of

skilled professionals will continue to challenge the industry and may prompt incentivization of STEM education and training by both the electronics firms and governments.

Sales methodologies also must continue to adapt to future changes. Changes underway include full and partial system fabrication services, hardware and software production and installation as a service, and innovative system integration support. Each requires multidisciplinary support from many industries, cooperating to deliver products in response to customer demands. Also, this will require cooperation between channel partners and in some cases agreements between industry competitors for success. Concepts, including “software-as-a-service” and “pay-for-what-is-used” may dominate electronics sales versus monolithic installation of applications on stand-alone systems and fixed-pricing of computer application and storage services. “Successful players will be those in the market with the capability to provide modular solutions that interlink products with security, software, and system consulting services.”⁶⁰

The U.S. electronics industry is trending toward both continued profitability and stiff competition from China and other international players. The challenges of security and continuously expanding the consumer base for electronics worldwide will drive innovation and changes in U.S. government policies and business practices to meet these market demands.

GOVERNMENTAL ROLES AND POLICY RECOMMENDATIONS

The U.S. government has three primary roles when interacting with any industry: as a buyer, sponsor, and regulator. These governmental roles vis-à-vis the electronics industry can both complement and contradict each other, and policymakers have struggled to balance competing imperatives while maximizing benefits and minimizing trade-offs. These efforts have entailed fostering innovation, offering incentives, and ensuring the supply of trusted critical electronics without distorting markets, while at the same time protecting national security without damaging American competitiveness and imposing unnecessary bureaucratic burdens. The United States enjoys many advantages in the global electronics marketplace but must implement proactive and innovative policies to maintain its strong position in the coming decades.

U.S. Government as Sponsor:

U.S. government policies should create an environment in which the electronics industry can flourish, increase global market share, and ultimately help increase the U.S. gross domestic product (GDP). Our research indicates that IP in product design and manufacturing processes is the crown jewel of the U.S. electronics industry. As such, government policies should strive to protect and foster future development of this asset. While existing policies support workforce education and encourage direct investment in developing technologies, the government needs to adopt new approaches and initiatives to help the U.S. electronics industry address emerging challenges.

Workforce: Approximately half of U.S. electronics engineers and scientists will reach retirement age in the next ten years.⁶¹ The United States derives significant advantages from intellectual capital built by its educational system. The United States should rebuild its STEM workforce through revitalized primary school outreach and sponsorship of secondary and tertiary education STEM programs with follow-on opportunities at the national labs. Additionally, the government should incentivize high-tech private companies to increase STEM internship and employment opportunities.⁶² A strong STEM workforce has spillover effects for other high-tech

industries and restricted government research programs.⁶³

Incentives: Congress should create better tax incentives for existing and emerging high-tech electronics companies. Attracted by single-digit tax burdens, some 700 U.S.-owned companies currently are headquartered in Ireland and contribute over \$300 billion annually to that country's GDP.⁶⁴ Permanently lowering tax rates could help attract high-tech investment and provide greater capital flexibility for companies to compete against heavily subsidized foreign competitors in a capital-intensive industry. More specifically, the government should implement tax and regulatory policies to incentivize on-shore fab construction. Because the electronics industry must navigate complicated and restrictive environmental, trade, and export regulations, narrowly applied exceptions or incentives in these areas would likely yield positive results for government access and assurance challenges.

Environment: The government also should invest in innovation and invention through public-private partnerships in the advanced manufacturing and electronics industries—such as Manufacturing U.S.A—which brings together academic, industrial, and governmental partners in synergetic innovation clusters.⁶⁵ The government should expand these programs to create self-reinforcing systems, capitalizing on government funding, unique intellectual capital, and expertise in commercialization. Expanding the Defense Advanced Research Projects Agency (DARPA) and the Intelligence Advanced Research Projects Activity (IARPA) would build additional capacity for innovation, benefiting both the public good and national security. In addition, Congress should authorize and fund the Manufacturing Advanced Research Projects Agency (MARPA), a new organization dedicated to tackling the growing challenges of electronics manufacturing.

Fostering New Markets: The government should help to create a new market by expanding sponsorships of flexible semiconductor fabrication technology projects. The flexible fab would have the capability to build high-mix, low-volume production to overcome difficulties of obsolescence and enhance manufacturing ranging from state-of-the-practice through state-of-the-art. Additionally, the government should continue to heavily invest in nascent microelectronic technologies to ensure “access and a healthy U.S. Industrial base.”⁶⁶ The government should extend DARPA's Common Heterogeneous Integration and Intellectual Property (CHIPS) effort to create reusable and trusted IP blocks.⁶⁷

U.S. Government as Buyer:

The U.S. government—and in particular the DoD—was a significant buyer of early electronics technology. Due to the globalization of electronics technology and its penetration into every aspect of daily life, the DoD is now responsible for less than 1 percent of the global market. The U.S. government should employ alternate strategies and policies to acquire what it needs from the market. The government should also reform the acquisition regulations to improve efficiency and shorten the program length from inception to fielding and implement systems to synchronize electronics requirements across programs. Finally, the government should provide more funding predictability.

Acquisition Reform: U.S. government and DoD acquisition programs take too long. For example, the V-22 Osprey program began in 1983 and did not achieve viable operations for almost three decades.⁶⁸ In contrast, the electronics industry is modernizing at a blistering pace, and state-of-the-art technology nodes are obsolete in five years. The current DoD effort to delegate acquisition program authority down to the O-5/O-6 level likely will remove significant barriers to progress. Another key to accelerating acquisitions is empowering program managers

to work with industry from the beginning to develop long-term and firm requirements. Minimizing program changes also would help avoid negative schedule impacts in later phases of the acquisition.

The government should explore areas of common interest with the commercial sector. Longstanding DoD specifications have made design and production of electronics for the military an unprofitable venture for contractors. Unique designs reduce DoD access to leading-edge microelectronics and increase the price with limited competition. For example, the DoD should leverage where possible commercial design standards for security to take advantage of businesses now leading in security protocols in most design applications. The Institute for Defense Analysis (IDA) concluded that the “DoD should make use of commercial manufacturing process flows, and ideally look and act like a commercial customer.”⁶⁹

Weapon System and Procurement Coordination: The DoD should gain better access to the electronics industrial base by coordinating specifications across multiple weapon systems. The electronics industry relies on high volume production to be profitable. DoD’s low microchip demand significantly decreases the number of contractors willing to compete the work, thus increasing the final cost. To combat this trend “the government should aggregate its IC needs as much as possible. This would mean coordinating procurements across the Services and programs.”⁷⁰ If the U.S. government were to synchronize technology development and procurement across multiple programs, there could be efficiencies gained through the initial system fielding, required maintenance, and lifetime buy replacements.

Obsolescence Planning: In order to maximize the duration of availability, programs should forecast the convergence of system-level technology readiness with commercial device architecture development (i.e., Moore’s law) and if possible anchor the architecture to a prolific commercial one. DoD programs also should budget for end-of-life buys and strategic stockpiling of critical electronic components.

Predictability: The government should establish more predictable DoD budgets, particularly in the Research, Development, Technology, and Experimentation (RDT&E) and procurement appropriations. Committing to multiyear budgets would allow the government to secure more stable contracts with companies developing technology. Current annual budgets create risk for contractors on the status of funding for multiyear programs, which translates into additional front-loaded costs and disincentive for independent R&D. Greater budget stability would give contractors more security and potentially lower costs. Most importantly, budget stability could secure more consistent industry support.

U.S. Government as Regulator:

The government should use regulatory, economic, and diplomatic tools to prevent, disrupt, and delay unauthorized exploitation of advanced U.S. electronics. Policies should limit access by current and potential adversaries while facilitating U.S. global competitiveness and trade with allies and partners. More than 80% of sales of U.S. semiconductor companies are to customers outside the United States, and U.S.-based firms account for almost half of the global market share.⁷¹ To ensure access to global markets and a level playing field while protecting national security interests, the U.S. government should pursue the following policies:

Take a comprehensive approach to reviewing foreign investment in and access to U.S. technology: Congress should expand the scope and authorities of the Committee on Foreign Investment in the United States (CFIUS). CFIUS currently does not cover many types of technology transfer which have the potential to damage national security. Examples include joint

ventures where the U.S. company contributes IP/technology rather than an entire business, private company transactions that are “below the radar,” minority investments that do not rise to the level of a “controlling interest,” reverse mergers, greenfield investments, and assets purchased from bankruptcies.⁷² Moreover, CFIUS has the authority and resources to review proposed transactions only on a case-by-case basis rather than taking a more comprehensive view of the entire technology landscape. This approach risks incremental damage to the entire electronics industry. Proposed legislation, the Foreign Investment Risks Review Modernization Act (FIRRMA), aims to address these shortcomings.⁷³ Congress and the President should pass and sign this legislation into law and fully fund its implementation.

Increase transparency, establish norms, and strengthen rule enforcement for international trade, intellectual property protection, and inward investment: Collaboration with allies in bilateral and multilateral forums—especially involving China—is essential to level the global market playing field and to protect critical IP.⁷⁴ Such efforts should include upholding anti-dumping laws and implementing effective anti-dumping remedies. The U.S. government also should help expand access to global markets by working with trade partners to reduce tariffs and other market access barriers (e.g. nontariff barriers to IC products with commercial/mass market encryption).⁷⁵

Attract and retain skilled immigrants in STEM Fields: One of the most common refrains heard from electronics industry interlocutors was the challenges in satisfying their needs for highly skilled labor in STEM fields solely from the available pool of U.S. citizens. The U.S. government should respond to industry's demands and capitalize on the strength of America's system of higher education by increasing the number of H1B and permanent resident visas. The United States should not only attract the best and brightest STEM students from around the world but also retain them in the U.S. workforce.

Reduce the risk of counterfeit semiconductors: The government should reduce counterfeit semiconductor risk by strengthening enforcement, increasing government-industry partnerships, and establishing norms and rules for electronic waste (e-waste) both domestically and internationally. Counterfeiters reuse, remark, and resell a significant portion of the millions of tons of e-waste produced and circulated across the world annually.⁷⁶ As a complement to efforts to detect counterfeit parts in military and government supply chains, the U.S. government can address the problem on the front end by strengthening the regulation of the domestic disposal and export of e-waste. This also would entail working with trade partners to establish multilateral norms and rules.

Evolve the Trusted Foundry Program to better balance supply chain risks: The Trusted Foundry Program trades reductions in assurance risk for increases in access risk within the supply chain. DoD needs to strike a better balance between risks to access and supply chain disruption and those associated with assurance/trust against counterfeit devices or malicious insertions. DoD should evolve the Trusted Foundry Program to better manage supply chain risk, consistent with the Microelectronics Innovation for National Security and Economic Competitiveness (MINSEC) strategy, including potential expansion of trusted foundries in NATO and major non-NATO allied countries. DoD should also continue to expand threat countermeasure programs, such as design obfuscation, component marker tagging and tracking, and imaging/forensics for inspection and verification.

By reforming policies and providing additional capital investments and incentives, the U.S. government can optimize its roles as sponsor, buyer, and regulator. The government should sponsor the whole gamut, from invention and innovation through the development,

commercialization, and sustained assured access of trusted microelectronic components for national security systems. In addition to completing acquisition and procurement reforms to reinvigorate its influence on industry as a buyer, the government should increase its adaptability and agility as a regulator to protect U.S. national security without hampering economic competitiveness and growth.

CONCLUSION

The electronics industry is healthy. Over the past 20 years, U.S. firms have consistently held a 50% revenue market share. The overall five-year forward-looking compound annual growth rate is 8%, with explosive growth anticipated for new product segments in AI, cognitive computing, and IoT. Nonetheless, our research indicates that the industry faces significant challenges. Trends toward consolidation and disaggregation continue to shift the industry's center of gravity from America toward Asia, particularly with respect to physical manufacturing. Yet based on our research, the crown jewel for U.S. companies is IP in product design and manufacturing processes. We recommend that these areas be protected and fostered above all else.

Governmental and industrial electronics challenges are not aligned with each other, and the U.S. government wields little market influence to compel industry to meet its needs for access, availability, and assurance. To make matters worse, industry views the U.S. government as a difficult customer, further lowering incentives to address governmental needs and challenges. With U.S. government demand comprising less than 1% of the total market, industry surge capacity in times of crisis or war may not be a concern, but industry's willingness to address unique governmental product and supply chain security requirements is.

The U.S. electronics industry's continued technological edge, competitiveness, integrity, and reliability is imperative for our national security and economic growth. Electronic components in weapons, communications, intelligence, and other defense and national security systems give U.S. and allied warfighters crucial advantages across all domains. Future advances in electronics and complementary technologies such as AI and autonomous systems promise to radically transform not only the nature of warfare but also fundamental aspects of civil society and the global economy. To secure these advantages and advances for current and future generations, the U.S. government must simultaneously perform several balancing acts, incentivizing R&D and intervening in markets without counterproductively distorting them, managing supply chain risks of both access and assurance while ensuring availability, and protecting critical IP without stifling economic growth and competitiveness. Based on an analysis of current industry conditions, challenges, and outlook, this study has recommended ways to achieve these goals and objectives by building on existing policies, programs, and initiatives and creating new ones.

ESSAYS

ESSAY 1: DoD's Trusted Foundry Program Challenges and Potential Solutions

In June 2003, Senator Joseph Lieberman submitted a white paper for Congressional record sounding the alarm on an imminent national security threat. Citing foreign government actions that capitalized on the globalization of the semiconductor industry, with specific emphasis on China, Senator Lieberman expressed concern that if the migration to East Asia continued, the DoD and intelligence agencies would lose first and assured access to the secure, advanced, chip-making capability needed to maintain the nation's technological edge.⁷⁷ The Senator's call to action included several recommendations, some of which the DoD implemented in an effort to maintain trusted sources for semiconductors. The DoD's trusted foundry program and other efforts to maintain this segment of the industrial base, however, did little to stem the wider trends and continued globalization of the industry. This essay will describe the evolution and current status of the trusted foundry program and provide recommendations to both set the conditions for continued U.S. competitiveness in the semiconductor industry and achieve DoD objectives of access, assurance, and availability of leading edge electronics for defense and intelligence programs.

History of the Trusted Foundry Program: Following Senator Lieberman's white paper, Deputy Secretary of Defense Paul Wolfowitz issued a memorandum in November 2003 titled "Defense Trusted Integrated Circuit Strategy," directing the DoD to develop a comprehensive strategy for procurement of trusted microelectronics that maximized competition, preserved a healthy domestic electronics industrial base, and ensured access to next-generation technology.⁷⁸

In 2004, the Under Secretary of Defense for Acquisition, Technology, and Logistics (U.S.D(AT&L)) took action by initiating a trusted foundry program in conjunction with the National Security Agency (NSA). Originally consisting of a single sole-source contract with the IBM Corporation to manufacture leading-edge defense microelectronics in a trusted environment, the program was expanded in 2007 to include a security accreditation program under the Defense Microelectronics Activity (DMEA) to assess and accredit suppliers under a wider array of activities. These activities included "design, aggregation, brokerage, mask manufacturing, foundry, post processing, packaging/assembly, and test services."⁷⁹ This greatly expanded the program,⁸⁰ achieving DoD objectives of integrity in integrated circuit (IC) design and production while also protecting critical intellectual property (IP) from potential adversaries. IBM, however, remained the only source of leading edge semiconductors.

In 2009, Congress again focused attention on trust in defense microelectronics, directing the DoD in Section 254 of the 2009 National Defense Authorization Act (NDAA) to establish a strategy for managing risk in the electronics supply chain and implement policies and actions to assure trust in ICs.⁸¹ The DoD initially responded in December 2009 on progress in implementing what was then called a Strategy for Systems Assurance and Trustworthiness,⁸² following up in 2012 with Department of Defense Instruction (DODI) 5200.44, implementing the Trusted Systems and Networks (TSN) strategy. This strategy emphasized a strong systems engineering approach to provide assurance for mission critical components consistent with the criticality of the system and manage risk in trust throughout the lifecycle of a program. It also mandated that defense-specific ASICs be produced in a DMEA accredited trusted foundry.⁸³

The sole-source trusted foundry arrangement with IBM provided for leading edge ASIC production through 2015. At that point, and as part of a period of widespread industry consolidation, IBM sold their foundry operations to Global Foundries, a firm owned by the United Arab Emirates.⁸⁴ The Committee on Foreign Investment in the United States (CFIUS)

reviewed and approved this sale and the U.S. based subsidiary of Global Foundries (GF) received DMEA accreditation and assumed IBM's contractual obligations. However, the continuing migration of the semiconductor fab industry and the GF status as a foreign-owned entity again created long-term uncertainty for the DoD. DMEA awarded a new long-term contract to GF in 2016, yet defense acquisition leaders advised DoD programs to execute life-time buys of production ready parts due to the long-term uncertainty of access.⁸⁵ As a result of the sale, Congress again requested a strategy in Section 231 of the 2017 NDAA, this time focusing not only on the DoD strategy for procuring from trusted sources, but also on a whole of government approach to maintain U.S. competitive advantage in electronics.⁸⁶ The DoD introduced this new comprehensive strategy in 2017 as Assuring Microelectronics Innovation for National Security and Economic Competitiveness (MINSEC). This strategy consists of two broad principles: 1) Generate and protect IP and U.S. competitiveness through enhancement of the U.S.-based semiconductor ecosystem, and 2) Invest in disruptive R&D to develop materials, devices, architectures, and design tools for next generation computing, strategic applications, and fabrication.⁸⁷

Conclusions from Industry Studies: Since the release of Senator Lieberman's white paper in 2003, multiple government, industry, and think tank organizations have conducted studies on the U.S. semiconductor industry and implications for national security. In addition to DoD reports required by the 2009 and 2017 NDAs, these include a Defense Science Board (DSB) Report in 2005,⁸⁸ a Government Accountability Office (GAO) Report in 2015,⁸⁹ the Fiscal Year 2016 Annual Industrial Capabilities report to Congress,⁹⁰ a 2016 Institute for Defense Analyses (IDA) Report,⁹¹ and 2017 reports by the President's Council of Advisors on Science and Technology (PCAST)⁹² and the National Defense Industrial Association (NDIA)⁹³ to name a few. Including the original Lieberman white paper, the reports are remarkably consistent in findings and conclusions can be summarized around three broad themes. First, the semiconductor industry has never been fully market driven, from original U.S. government investments that led to the invention of the transistor and integrated circuit, to China's subsidies of its domestic industry today. Market forces and U.S. innovation alone, therefore, cannot ensure the survival of a domestic semiconductor manufacturing capability. Second, the semiconductor industry is now highly globalized and driven by the consumer electronics market. With defense requirements accounting for a small fraction of global electronics demand, the commercial market will not internally provide for all specialized needs of the defense and intelligence communities. Third, a vibrant electronics industrial ecosystem should be considered a national strategic priority. This will require a long-term strategy, whole of government approach, and sustained funding.

Recommendations: From the start of the trusted foundry program in 2003, the DoD and intelligence community have worked closely in implementing a strategy for assured access to trusted microelectronics, adjusting that strategy as conditions changed. As an example, the DoD is currently doing a Field Programmable Gate Array (FPGA) assurance study to assess ways to ensure trust in this widely used type of IC, which is largely produced outside the U.S.⁹⁴ Clearly, though, the strategy as implemented did not prioritize the overall health of the domestic electronics ecosystem. Whether due to failure to anticipate the disintegration of the electronics value stream, an inability to marshal wider government support for a coordinated national strategy, or resourcing simply insufficient to achieve the desired ends, the path forward is clear if also complex. The U.S. should now prioritize having a vibrant domestic electronics industrial base as a strategic end. Our recommendations are based accordingly.

First, the DoD needs a comprehensive strategy, developed in coordination with other government agencies, to maintain U.S. competitiveness in IC design and production. This includes focused R&D on systems security engineering and secure circuit design methods in support of new computing paradigms such as quantum computing.⁹⁵ It also includes adjusting the tax and regulatory structure to increase the attractiveness of the U.S. as a fab location. The 2018 Tax Cuts and Jobs Act, which cuts corporate tax rates from 35% to 21%, is a start, but still represents a significant headwind as compared to countries that subsidize their electronics industries. The strategy should include ways to foster public-private cooperation akin to SEMATECH⁹⁶ in the 1980s, and encourage other critical industries such as infrastructure, finance, and the wider national security community including U.S. partners and allies to adopt trust requirements.⁹⁷ The strategy should also identify national development priorities, such as moonshot recommendations advocated by PCAST,⁹⁸ or a fully resourced 10-year plan.⁹⁹

Second, the DoD should take both short and long-term actions to ensure access to trusted sources of leading edge semiconductors for defense needs. In the short term, this includes finding another trusted source beyond GF. This can be an existing U.S.-based facility such as the State University of New York Poly SEMATECH, another existing U.S. fab with leading edge capability (Intel), or a fab in an allied or partner nation. Short-term actions should also include continued use of FPGAs as well as efforts to assure trust for both hardware and software. In the long term, the DoD needs to develop a technology roadmap that identifies critical technology nodes to include semiconductor geometries and processes. Programs should be coordinated and developed around these nodes as a way of achieving better economies of scale, with allies and partners included. Development of national priorities or moonshot goals would aid in this approach. The DoD should also develop alternative ways of verifying components for which a trusted foundry is not available.¹⁰⁰

ESSAY 2: Expanding the Access and Assurance Challenge

The Access Challenge: General Joseph Dunford, Chairman of the Joint Chiefs of Staff, testified to Congress in September that he believes “China probably poses the greatest threat to our nation by about 2025.”¹⁰¹ Viewing the electronics industry through this lens reveals access as a primary risk to national security. This challenge stems from a combination of the fully globalized industry creating critical system nodes in potentially geopolitically contentious regions (Asia-Pacific) that the U.S. may not be able to access in the event of conflict with China.

As of 2015, 84% of the world’s semiconductor fabrication capacity (Table 1) is located in the Asian-Pacific region.¹⁰² The move of fabrication capacity is well-entrenched and unlikely to move back to the U.S. even with aggressive policy changes.

The U.S. does still maintain world leadership in areas of “fabless” semiconductor work (the creative design and programming aspects of the industry) as well as fabrication manufacturing equipment; however, those areas are also at risk of offshore migration (primarily due to lack of STEM skill sets in the U.S. workforce). This fully globalized and specialized dynamic has resulted in a situation in which no firm or nation currently has the capacity to serve consumer (or



national military) demand solely using assets within its own borders.

While the U.S. is highly reliant on Asian fabrication (see table 2), others around the globe are just as reliant on our intellectual property (“fabless” design) and manufacturing equipment. As it currently stands, this fully globalized industry actually presents a strength in major conflict deterrence in that the prosperity and security of all nations involved is inextricably interdependent. The risk to U.S. national security only manifests when layered with stated goals and known investments made by the Communist Party of China.

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

Table 2 - Global Wafer Capacity

“In June 2014, the State Council of China released the National Guidelines for Development and Promotion of the Integrated Circuit (IC) Industry ... with goals to increase its self-sufficiency rate for integrated circuits to 40 percent by 2020 and to 70 percent by 2025”¹⁰³

To meet this goal, China made an estimated \$55B investment in fabrication facilities in its previous five-year plan (see figure 2). China has made similar policy goals and financial investments in both capital-intensive intellectual capabilities and manufacturing equipment capabilities. All of these actions lead to the true risk and challenge presented to the DoD. What happens to the DoD supply chain and capabilities if China truly gains self-sufficiency, gains complete freedom of geopolitical action through that self-sufficiency, and decides to act aggressively to isolate the U.S. from the Pacific supply chain? The likely answer is that the DoD would not be able to execute a long-duration conflict without major mobilization of U.S. based fabrication. The average construction timeline for a semiconductor fabrication facility is approximately two years from low to high volume production, making a fresh-start policy unrealistic. Construction of standing arsenal-type government fabrication facilities makes very little sense in that technology innovation moves more rapidly that government processes would ever be able to sustain in a financially viable way. The two most viable solutions are 1) fostering an environment in the U.S. that makes it commercially appealing to bring fabrication facilities back to the United States; and 2) developing plans, policies and agreements with the major U.S. fabrication facilities (Trusted Foundries, Intel, Micron, etc). Both solutions would prioritize supply of DoD materials, in the time of war, including detailed plans on adapting currently commercial operations to suit DoD needs similar to the arrangements made with industry during WWII.



The Assurance Challenge: With the end of the Cold War in the 1990’s and the Global War

on Terrorism in the 2000's, the nation fell into a false sense of security.¹⁰⁴ Technology advanced quickly with tremendous profits leaving little concern about vulnerabilities. Only until recently, the biggest perceived threat by the government was a terrorist attack from a violent extremist group. These threats could be managed with traditional operational security measures. The United States government (federal, state, and local) is now heavily reliant on electronics because the benefits have outweighed the risks of the past.

The microelectronics industry has a very extensive and intertwined ecosystem that must rely on each other to be successful.¹⁰⁵ The electronics ecosystem must also be collectively assessed and disaggregated individually to address the multiple security related vulnerabilities from the supply chain and IC development to end user markets. As previously mentioned in this paper, there are significant concerns about the electronics supply chain given the access and availability of strategic materials and quality components used in semiconductor manufacturing. The government, for example, is very concerned about the overall microelectronic supply chain (hardware and software) and network security. However, the government is addressing “cybersecurity” concerns disproportionately and decentralized across agencies at the federal, state, and local levels. Each agency has its own cyber security related resource, which do not synchronize or integrate activities across the government.

Collaboration with civilian industry is sporadic and isolated, focused primarily on software vulnerabilities or consequence management in the event of a major cyber related attack.¹⁰⁶ Industry, on the other hand, is less concerned about hardware or the supply chain citing the security vulnerabilities are introduced primarily from the software perspective. For example, leaders in the electronics industry claim they have not experienced significant loss of revenue due to hardware security concerns.¹⁰⁷ The industry states that IC development is closely managed and tested at every phase to ensure reliability to the customer. The government believes weaknesses are at every phase, especially at the chip design phase.

Globalization has increased opportunities and associated vulnerabilities. Neither the government, nor industry, can afford to meet its goals without having to rely on outsourcing to foreign entities to meet its needs. Despite all of these concerns, the government and industry continue to invest billions of dollars on R&D, human capital, and other technological initiatives only to have policies and regulations constrain the overall growth of the electronics industry in the United States. Therefore, in order to promote assurance in the electronics industry, better collaboration and understanding among all stakeholders are in order—in addition to the policy recommendations above—to maintain momentum with emerging technologies.

ESSAY 3: Quantum Computing

While the U.S. enjoys unparalleled dominance in semiconductor architecture, quantum computing has the potential to disrupt the existing microelectronics market by creating microchips with more computing power than the world's fastest conventional supercomputers. In March 2018, Google announced the world's fastest known quantum computer, Bristlecone, with a 72 qubits core processor.¹⁰⁸ Qubits, or quantum bits, are not scalable to traditional computer processing speeds. Google believes they have achieved quantum supremacy, the point which quantum computers surpass today's fastest traditional supercomputers.¹⁰⁹ In fact, “a quantum computer with just a few hundred qubits would be able to perform more calculations simultaneously than there are atoms in the known universe.”¹¹⁰ However, quantum computing is not currently a direct replacement for existing computer technology primarily because of the tightly controlled conditions required for operation. Quantum computers only operate at

extremely low temperatures, around negative 460 degrees Fahrenheit, to isolate the processor from all external vibrations.¹¹¹

The technology is not ready yet for significant scaling and implementation, but eventually 100,000-qubit systems are envisioned.¹¹² The possibility of significant quantum computing systems means tremendous market potential. The global market is already over \$88 billion and growing at a compounded annual growth rate of 29.1 percent.¹¹³ Existing supercomputers soon will use quantum computers as accelerators to solve currently unsolvable problems. The computing power will lead to significant disruptions across multiple industries, including “materials, chemistry, and drug,” by building “accurate molecular-scale models” and accelerating innovation.¹¹⁴ Additionally, quantum computing has multiple national defense applications, including cryptography, secure communications, AI, extremely accurate gravity sensing that could remotely detect tunnels or submarines, and timekeeping as much as 1,000 times more accurate than GPS.¹¹⁵

ESSAY 4: Export Control

Discussed for many years and finally launched in 2009, the Export Control Reform (ECR) initiative aimed to put “higher fences around the most sensitive items” while liberalizing controls on the least sensitive hardware and technology.¹¹⁶ This entailed collaboration among the Departments of State, Commerce, and Defense to move specific defense articles from the United States Munitions List (USML) to the less restrictive Commerce Control List (CCL) while rewriting the USML to make its descriptions of controlled items and technology more specific. Regulators largely completed this process in 2016 and immediately started re-reviewing and revising the USML and CCL as planned, in order to keep up with changing technology – both loosening restrictions on items that are no longer sensitive and placing restrictions on emerging technologies with critical national security implications.

Unfortunately, the pace of much of this work has slowed during the transition to a new administration, which has included leadership and staffing vacancies, freezes on hiring and lateral transfers, and regulatory reviews. In addition, some electronics industry representatives who spoke to the seminar asserted the U.S. government—and in particular, the DoD's Defense Technology Security Administration (DTSA)—continues to damage U.S. competitiveness by restricting technologies without regard for international availability.

The U.S. government should take several steps to address this situation. The Executive Branch should rebuild and fully staff the relevant regulatory offices in the Departments of State and Commerce and complete the regulatory reform. Also, the Department of State should redouble its efforts in bilateral and multilateral forums to establish international norms and rules to apply uniform export controls to level the playing field for U.S. companies. Congress should adequately fund those agencies and exercise additional oversight over the USML and CCL to ensure U.S. economic interests remain competitive. Recently proposed bipartisan legislation, the Export Control Reform Act of 2018, may overly restrict technology in an attempt to address the legitimate need to protect U.S. technology against exploitation.¹¹⁷ Instead of continuing to tinker with the existing patchwork of disjointed export control authorities, Congress should complete ECR's previously planned final phase, which envisioned a unified regulatory system consisting of “four singles”: a single control list, a single licensing agency, a single information technology system, and a single enforcement coordination center.¹¹⁸ Overcoming entrenched interests and bureaucratic turf wars will be a tall order, but the gains in transparency, consistency, simplicity, and efficiency are worth the expenditure of effort and political capital.

-
- ¹ Semiconductor Industry Association, *2017 Factbook*, Washington, DC, (May 2017): 2.
- ² PR Newswire, “Global Semiconductor Market Forecast 2017-2024,” (October 23, 2017), accessed April 4, 2018, <https://www.prnewswire.com/news-releases/global-semiconductor-market-forecast-2017-2024-300541299.html>.
- ³ Databeans, “2017 Semiconductor Military and Aerospace Applications,” accessed April 4, 2018, <https://www.databeans.net/downloads/category/reports/semiconductors-in-military-aerospace-applications/>.
- ⁴ Office of the Deputy Assistant Secretary of Defense for Manufacturing and Industrial Base Policy, “Report to Congress, Fiscal Year 2016, Annual Industrial Capabilities,” Washington, DC, (March 2017): 38.
- ⁵ Semiconductor Industry Association, *2017 Factbook*: 10.
- ⁶ Ibid: 5.
- ⁷ Michaela D. Platzer and John F. Sargent, Jr., “U.S. Semiconductor Manufacturing: Industry Trends, Global Competition, Federal Policy,” Congressional Research Service, (June 27, 2016): 4.
- ⁸ Ibid: 6.
- ⁹ Ibid.
- ¹⁰ Wikipedia, “Moore’s Law,” updated March 27, 2018, accessed March 31, 2018, https://en.wikipedia.org/wiki/Moore%27s_law.
- ¹¹ Charles King, “Moore’s Law is Golden”, *Computerworld* (21 April 2015), accessed 4 May 2018, <http://www.computerworld.com/article/2912683/computer-processors/moore-s-law-is-golden.html>.
- ¹² TSMC says latest chip plant will cost around \$20 bln, Reuters, access 4 May 2018, <https://www.reuters.com/article/tsmc-investment/tsmc-says-latest-chip-plant-will-cost-around-20-blnd-idUSL3N1O737Z>.
- ¹³ Radack, Cohen, Leheny, Sharma, and Slusarczuk, *Semiconductor Industrial Base Focus Study-Final Report: 1-2*.
- ¹⁴ IC Insights, “Global Wafer Capacity 2018-2022,” (January 2018), accessed March 23, 2018, www.icinsights.com/data/reports/5/0/brochure.pdf?parm=1521815104
- ¹⁵ Semiconductor Industry Association, *2017 Factbook*: 15.
- ¹⁶ Ibid: 19.
- ¹⁷ Ibid: 3.
- ¹⁸ Platzer and Sargent, Jr., “U.S. Semiconductor Manufacturing: Industry Trends, Global Competition, Federal Policy:” 6.
- ¹⁹ IC Insights, “Global Wafer Capacity 2018-2022.”
- ²⁰ Platzer and Sargent, Jr., “U.S. Semiconductor Manufacturing: Industry Trends, Global Competition, Federal Policy:” 6.
- ²¹ Robert C. Leachman and Chien H. Leachman, “Trends in Worldwide Semiconductor Fabrication Capacity,” Engineering Systems Research Center, University of California, Berkeley, CA, (July 22, 1999): 7.
- ²² Semiconductor Industry Association, “SIA 2017 Factbook,” accessed April 1, 2018, 3, www.semiconductors.org/industry_statistics/.
- ²³ Michaela D. Platzer and John F. Sargent Jr., *U.S. Semiconductor Manufacturing: Industry Trends, Global Competition, Federal Policy*, CRS Report for Congress R44544, (Washington DC: Congressional Research Service, June 27, 2016), 11, https://www.everycrsreport.com/reports/R44544.html#_Toc454871190.
- ²⁴ Brian S. Cohen, “DOD Integrated Circuit (IC) Supply Chain Issues,” (PowerPoint presentation, Institute for Defense Analyses, Alexandria, VA, February 21, 2018).
- ²⁵ Accredited Suppliers,” Trusted Foundry Program, *Defense Microelectronics Activity*, last updated March 30, 2018, <https://www.dmea.osd.mil/otherdocs/AccreditedSuppliers.pdf>.
- ²⁶ Dan Rosso, “Annual Semiconductor Sales Increase 21.6%, Top \$400 Billion for First Time,” News, *Semiconductor Industry Association*, February 5, 2018, www.semiconductors.org/news/.
- ²⁷ SIA Factbook 2017, 12.
- ²⁸ Jeremy Muldavin, “Assuring Microelectronics Innovation for National Security & Economic Competitiveness (MINSEC),” (PowerPoint presentation, Office of the Deputy Assistant Secretary of Defense for Systems Engineering, Washington DC, November 29, 2017).
- ²⁹ SIA and Nathan Associates, *Beyond Borders: The Global Semiconductor Value Chain*, May 2016, 23.
- ³⁰ Cohen, “DOD Integrated Circuit (IC) Supply Chain Issues,” 20.
- ³¹ Jeremy Muldavin, “Assuring Microelectronics Innovation for National Security & Economic Competitiveness (MINSEC),” 2.
- ³² GlobalFoundries, “GLOBALFOUNDRIES Completes Acquisition of IBM Microelectronics Business,” *GlobalFoundries.com*, July 1, 2015. <https://www.globalfoundries.com/news-events/press-releases/globalfoundries-completes-acquisition-of-ibm-microelectronics-business>.

- ³³ Michael E. Porter, “The Five Competitive Forces that Shape Strategy,” *Harvard Business Review* (January 2008): 79-93.
- ³⁴ SIA Factbook 2017, 15.
- ³⁵ SIA Factbook 2017, 14.
- ³⁶ Defense Microelectronics Activity, “Trusted Supplier Accreditation Process,” *DMEA*, April 2, 2018, https://www.dmea.osd.mil/docs/trusted_supplier_accreditation_process.pdf.
- ³⁷ SIA, *Beyond Borders*, 3.
- ³⁸ Platzer, U.S. Semiconductor Manufacturing: Industry Trends, Global Competition, Federal Policy, 6.
- ³⁹ Platzer, U.S. Semiconductor Manufacturing: Industry Trends, Global Competition, Federal Policy, 3-4.
- ⁴⁰ Cohen, “DOD Integrated Circuit (IC) Supply Chain Issues,” 34.
- ⁴¹ Platzer, U.S. Semiconductor Manufacturing: Industry Trends, Global Competition, Federal Policy, 15.
- ⁴² National Defense Industrial Association (NDIA) Trusted Microelectronics Joint Working Group, “Team 1 White Paper: Future Needs & System Impact of Microelectronics Technologies,” *NDIA.org*, July 2017, 10-11.
- ⁴³ Platzer, U.S. Semiconductor Manufacturing: Industry Trends, Global Competition, Federal Policy, 2, 6.
- ⁴⁴ Platzer, U.S. Semiconductor Manufacturing: Industry Trends, Global Competition, Federal Policy, 11.
- ⁴⁵ Platzer, U.S. Semiconductor Manufacturing: Industry Trends, Global Competition, Federal Policy, 10.
- ⁴⁶ Anthony Kimbery, “China’s Semiconductor Strategy is bad news for foreign companies” *Biometric Stocks*, *Biometric*, December 13, 2017. <https://www.biometricupdate.com/201712/chinas-semiconductor-strategy-is-bad-news-for-foreign-companies>
- ⁴⁷ President’s Council of Advisors on Science and Technology (PCAST), “Report to the President: Ensuring Long-Term U.S. Leadership in Semiconductors,” *Executive Office of the President*, January 2017, 8.
- ⁴⁸ Anthony Kimbery, “China’s Semiconductor Strategy is Bad News for Foreign Companies,” *BiometricUpdate.com*, December 13, 2017, accessed April 1, 2018, <https://www.biometricupdate.com/201712/chinas-semiconductor-strategy-is-bad-news-for-foreign-companies>.
- ⁴⁹ <https://www.mckinsey.com/global-themes/asia-pacific/a-new-world-under-construction-china-and-semiconductors>
- ⁵⁰ Villasenor, John, “Ensuring Hardware Cybersecurity,” *Brookings* (2011): <https://www.brookings.edu/research/ensuring-hardware-cybersecurity/>
- ⁵¹ IBISWorld, “IBISWorld Industry Report Global Semiconductor & Electronic Parts Manufacturing,” November 2017, 4.
- ⁵² Rajat Dhawan, Bernd Heid, Paul Küderli, and Kevin Laczkowski, “How industrial companies can respond to disruptive forces,” April 2018. Accessed April 8, 2018, <https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/how-industrial-companies-can-respond-to-disruptive-forces>.
- ⁵³ Tim Zanni, Lincoln Clark, Chris Gentle, and Scott Jones, “Semiconductors: Can the surge continue? Electric performance in 2017 powers tempered optimism - 2018 KPMG Global Semiconductor Industry Outlook,” *KPMG*, 2.
- ⁵⁴ IBISworld, 5.
- ⁵⁵ IBISworld, 9-10.
- ⁵⁶ “Chips on their shoulders,” *The Economist*, January 23, 2016, accessed April 8, 2018, <https://www.economist.com/news/business/21688871-china-wants-become-superpower-semiconductors-and-plans-spend-colossal-sums>
- ⁵⁷ Peter Clarke, “China startup releases AI processors then raises \$100 million,” *eeNews Europe*, April 4, 2018, accessed April 8, 2018, <http://www.eenewseurope.com/news/china-startup-releases-ai-processors-then-raises-100-million>
- ⁵⁸ Thierry Chesnais and Christopher Thomas, “How semiconductor companies can win in China’s new product-development landscape,” *McKinsey on Semiconductors*, Number 6 (April 2017): 32-33, accessed April 8, 2018, https://www.mckinsey.com/~media/McKinsey/Industries/Semiconductors/Our%20Insights/McKinsey%20on%20Semiconductors%20Issue%206%20-%20Spring%202017/McK%20on%20Semiconductors_Issue%206_2017.ashx.
- ⁵⁹ Jeff Dorsch & Ed Sperling, “IC Industry Waking Up To Security,” *Semiconductor Engineering*, June 2, 2016, accessed April 8, 2018, <https://semiengineering.com/ic-industry-waking-up-to-security/>.
- ⁶⁰ Grigori Bokeria, Matthias Frahm, & Sascha Rahman, “Future of the semiconductor industry: Profitable growth with new dynamic market trends,” *Simon-Kucher & Partners*, January 9, 2018, accessed April 8, 2018, <https://www.simon-kucher.com/es/blog/future-semiconductor-industry-profitable-growth-new-dynamic-market->

trends.

⁶¹ “A 21st Century Science, Technology, and Innovation Strategy for America’s National Security” (Committee on Homeland and National Security of the National Science and Technology Council, May 2016), 4, http://www.defenseinnovationmarketplace.mil/resources/National_Security_ST_Strategy_2016_FINAL.PDF.

⁶² “Team 1 White Paper: Future Needs & System Impact of Microelectronics Technologies,” Trusted Microelectronics Joint Working Group (National Defense Industrial Association, July 2017), 9, <https://www.ndia.org/-/media/sites/ndia/divisions/working-groups/tmjwg-documents/ndia-tm-jwg-team-1-white-paper-finalv3.ashx?la=en>.

⁶³ “Team 1 White Paper: Future Needs & System Impact of Microelectronics Technologies.”

⁶⁴ Simon Roughneen, “Ireland Has Become a Mecca for U.S. Tech Companies. Can Trump Lure Them Home?,” *LA Times*, February 10, 2017, online edition, sec. Europe, <http://www.latimes.com/world/europe/la-fg-ireland-economy-2017-story.html>.

⁶⁵ “Manufacturing U.S.A.,” About Us, accessed April 10, 2018, <https://www.manufacturingusa.com/pages/program-details>.

⁶⁶ “Team 1 White Paper: Future Needs & System Impact of Microelectronics Technologies,” 21.

⁶⁷ CHIPS aims “to develop a new technological framework in which different functionalities... can be segregated into small chiplets which then can be mixed and matched.” “Revolution at Full Speed Builds Its Own Momentum,” News and Events, DARPA’s Drive to Keep the Microelectronics Defense Advanced Research Projects Agency, August 25, 2017, <https://www.darpa.mil/news-events/2017-08-25>.

⁶⁸ “DOD Acquisition: Case Study of the Navy V-22 OSPREY Joint Vertical Lift Aircraft Program,” July 31, 1986, 2.

⁶⁹ Radack, Daniel J.; Brian S. Cohen; Robert F. Leheny; Vashisht Sharma; Marko M.G. Slusarczyk “Semiconductor Industrial Base Focus Study - Final Report”. Institute for Defense Analysis. Dec 2016. Pg v.

⁷⁰ Ibid.

⁷¹ 2017 Semiconductor Industry Association Factbook, <http://go.semiconductors.org/2017-sia-factbook-0-0-0>.

⁷² Michael Brown and Pavneet Singh, China’s Technology Transfer Strategy: How Chinese Investments in Emerging Technology Enable A Strategic Competitor to Access the Crown Jewels of U.S. Innovation, Defense Innovation Unit Experimental, January 2018, [https://admin.govexec.com/media/diux/chinatechnologytransferstudy_jan_2018_\(1\).pdf](https://admin.govexec.com/media/diux/chinatechnologytransferstudy_jan_2018_(1).pdf), 42-43.

⁷³ Statement by the Press Secretary Supporting the Foreign Investment Risk Review Modernization Act, The White House, January 24, 2018, <https://www.whitehouse.gov/briefings-statements/statement-press-secretary-supporting-foreign-investment-risk-review-modernization-act/>.

⁷⁴ Semiconductor Industry Association Letter to President Trump, November 30, 2016, [https://www.semiconductors.org/clientuploads/directory/DocumentSIA/GeneralResources/SIA%20letter%20&%20policy%20agenda%20Nov%202016%20new1\[2\].pdf](https://www.semiconductors.org/clientuploads/directory/DocumentSIA/GeneralResources/SIA%20letter%20&%20policy%20agenda%20Nov%202016%20new1[2].pdf)

⁷⁵ Ibid.

⁷⁶ Tom Sharpe, “E-Waste Export Controls Key to Battling Counterfeiters,” *National Defense Business and Technology Magazine*, March 2016, <http://www.nationaldefensemagazine.org/archive/2016/March/Pages/E-WasteExportControlsKeytoBattlingCounterfeiters.aspx>.

⁷⁷ Cong. Rec., 108th Cong., 1st sess., 2003, vol. 149, no. 82: 7468-71.

⁷⁸ U.S. Department of Defense, Department of Defense Assured Microelectronics Policy, Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, July 2014, 2.

⁷⁹ U.S. Department of Defense, Department of Defense Assured Microelectronics Policy, 3.

⁸⁰ “Accredited Suppliers,” Trusted Foundry Program, Defense Microelectronics Activity, last updated March 30, 2018, <https://www.dmea.osd.mil/otherdocs/AccreditedSuppliers.pdf>. The DMEA Trusted Foundry Program includes 75 accredited suppliers as of March 30, 2018.

⁸¹ National Defense Authorization Act for Fiscal Year 2009, Public Law 110-417, § 254, 110th Cong. (October 14, 2008).

⁸² U.S. Department of Defense, Executive Summary and Addendum, Report on Trusted Defense Systems in Response to National Defense Authorization Act (2009), Section 254, Under Secretary of Defense for Acquisition, Technology, and Logistics and Assistant Secretary of Defense for Networks and Information Integration/DOD Chief Information Officer, December 22, 2009, ii.

⁸³ U.S. Department of Defense, Department of Defense Instruction (DODI) 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN), November 5, 2012, Incorporating Change 2, July 27, 2017, 2-3.

⁸⁴ Testimony Before the United States House of Representatives Committee on Armed Services Subcommittee on

Oversight and Investigations, Witness Statement of Andre' Gudger, Kristen Baldwin, and Brett Hamilton, 114th Cong., 1st sess., October 28, 2015, 3.

⁸⁵ Kristen Baldwin, "Policy Perspective: The Current and Proposed Security Framework," (PowerPoint presentation, Office of the Deputy Assistant Secretary of Defense for Systems Engineering, Washington DC, August 16, 2016), 8.

⁸⁶ National Defense Authorization Act for Fiscal Year 2017, Public Law 114-328, § 231, 114th Cong. (December 23, 2016).

⁸⁷ Jeremy Muldavin, "Assuring Microelectronics Innovation for National Security & Economic Competitiveness (MINSEC)," 2, (PowerPoint presentation, Office of the Deputy Assistant Secretary of Defense for Systems Engineering, Washington DC, November 29, 2017).

⁸⁸ U.S. Department of Defense, Defense Science Board Task Force on High-Performance Microchip Supply, Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, February 2005.

⁸⁹ Marie A. Mak, Trusted Defense Microelectronics: Future Access and Capabilities are Uncertain, GAO Report GAO-16-185T, (Washington DC: Government Accountability Office, October 28, 2015).

⁹⁰ U.S. Department of Defense, Fiscal Year 2016 Annual Industrial Capabilities, Under Secretary of Defense for Acquisition, Technology, and Logistics and Deputy Assistant Secretary of Defense for Manufacturing and Industrial Base Policy, Report to Congress, March 2017.

⁹¹ Daniel J. Radack, "Semiconductor Industrial Base Focus Study – Final Report," Institute for Defense Analyses (IDA), December 2016, accessed April 10, 2018, 1-1, https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&ved=0ahUKEwic-dXIXrHaAhUL44MKHbf2AIYQFggxMAI&url=https%3A%2F%2Fwww.ida.org%2Fidamedia%2FCorporate%2Ffiles%2FPublications%2FIDA_Documents%2FITSD%2F2017%2FD-8294.ashx&usq=AOvVaw15hriiSx7LAjdXYnGYXYJh.

⁹² President's Council of Advisors on Science and Technology (PCAST), Executive Office of the President, Report to the President: Ensuring Long-Term U.S. Leadership in Semiconductors, January 2017, accessed April 10, 2018, https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_ensuring_long-term_us_leadership_in_semiconductors.pdf.

⁹³ National Defense Industrial Association (NDIA) Trusted Microelectronics Joint Working Group, "Team 1 White Paper: Future Needs & System Impact of Microelectronics Technologies," NDIA.org, July 2017, accessed April 10, 2018, <https://www.ndia.org/-/media/sites/ndia/divisions/working-groups/tmjwg-documents/ndia-tm-jwg-team-1-white-paper-finalv3.ashx?la=en>.

⁹⁴ Muldavin, 27.

⁹⁵ NDIA, 18.

⁹⁶ Clair Brown and Greg Linden, Chips and Change (Cambridge, MA: MIT Press, 2011), 20. SEMATECH was a research consortium of fourteen U.S. chip companies formed in 1987 in response to the growing Japanese semiconductor industry. The U.S. government relaxed antitrust laws affecting interfirm cooperation and provided half the \$200 million annual budget.

⁹⁷ Muldavin, 7.

⁹⁸ PCAST, 21-24.

⁹⁹ NDIA, 20.

¹⁰⁰ Muldavin, 27.

¹⁰¹ Ryan Browne, "Top U.S. general: China will be 'greatest threat' to U.S. by 2025", *CNN Politics*, September 27, 2017, <http://www.cnn.com/2017/09/26/politics/dunford-us-china-greatest-threat/index.html>.

¹⁰² Michaela D. Platter & John F. Sargent Jr., "U.S. Semiconductor Manufacturing: Industry Trends, Global Competition, Federal Policy," Congressional Research Service, June 27th 2016, <https://fas.org/sgp/crs/misc/R44544.pdf>.

¹⁰³ Christopher Thomas, "A new world under construction: China and semiconductors," McKinsey & Company, November 2015, <https://www.mckinsey.com/global-themes/asia-pacific/a-new-world-under-construction-china-and-semiconductors>.

¹⁰⁴ Harper, John, "China Threatens Microelectronics Supply Chain, DoD Official Says," *National Defense* (2017): <http://www.nationaldefensemagazine.org/articles/2017/12/19/china-threatens-microelectronics-supply-chain-dod-official-says#>.

¹⁰⁵ Discussion with electronics industry official, San Jose, CA, 4 April, 2018.

¹⁰⁶ Bronell, Michelle, Discussion with electronics industry official, San Jose, CA, 4 April, 2018.

¹⁰⁷ Bronell, Michelle, Discussion with electronics industry official, San Jose, CA, 5 April, 2018.

¹⁰⁸ Martin Giles and Will Knight, "Google Thinks It's Close to 'Quantum Supremacy.' Here's What That Really Means," *MIT Technology Review*, March 9, 2018, <https://www.technologyreview.com/s/610274/google-thinks-its->

close-to-quantum-supremacy-heres-what-that-really-means/.

¹⁰⁹ Martin Giles and Knight.

¹¹⁰ Russ Juskalian, “Advances at Google, Intel, and Several Research Groups Indicate That Computers with Previously Unimaginable Power Are Finally within Reach,” *Technology Review*, December 9, 2017, <https://www.technologyreview.com/s/603495/10-breakthrough-technologies-2017-practical-quantum-computers/>.

¹¹¹ Will Knight, “Serious Quantum Computers Are Finally Here. What Are We Going to Do with Them?,” *MIT Technology Review*, February 21, 2018, <https://www.technologyreview.com/s/610250/hello-quantum-world/>; Martin Giles and Knight, “Google Thinks It’s Close to ‘Quantum Supremacy.’ Here’s What That Really Means.”

¹¹² Juskalian, “Advances at Google, Intel, and Several Research Groups Indicate That Computers with Previously Unimaginable Power Are Finally within Reach.”

¹¹³ DataBridge Market Research, “Quantum Computing Market Research 2018: Region Wise Analysis of Top Players in Market by Its Types and Application,” *Herald Keeper*, March 22, 2018, <http://heraldkeeper.com/featured/quantum-computing-market-research-2018-region-wise-analysis-of-top-players-in-market-by-its-types-and-application-52085.html>.

¹¹⁴ Juskalian, “Advances at Google, Intel, and Several Research Groups Indicate That Computers with Previously Unimaginable Power Are Finally within Reach.”

¹¹⁵ “The Assistant Secretary of Defense for Research and Engineering’s Strategic Guidance” (ASD (R&E), May 1, 2018), 7,

[https://www.acq.osd.mil/chieftechologist/publications/docs/ASD\(R&E\)_Strategic_Guidance_May_2014.pdf](https://www.acq.osd.mil/chieftechologist/publications/docs/ASD(R&E)_Strategic_Guidance_May_2014.pdf).

¹¹⁶ Under Secretary Eric L. Hirschhorn Remarks, Trade Development Alliance of Greater Seattle, February 26, 2015, <https://www.bis.doc.gov/index.php/2011-09-12-15-56-29/2012-06-26-19-35-02/speeches-archives/173-about-bis/newsroom/speeches/speeches-2015/844-remarks-of-under-secretary-eric-l-hirschhorn-export-control-forum-newport-beach-california-3>. **See also** Ian F. Fergusson and Paul K. Kerr, *The U.S. Export Control System and the Export Control Reform Initiative*, Congressional Research Service, March 18, 2018, <https://fas.org/sgp/crs/natsec/R41916.pdf>.

¹¹⁷ Export Control Reform Act of 2018, H.R. 5040, U.S. House of Representatives, February 15, 2018, <https://foreignaffairs.house.gov/wp-content/uploads/2018/02/hr-5040.pdf>; *The Export Control Reform Act of 2018: Risks and Opportunities in the Modernization of U.S. Export Controls*, Clifford Chance, February 26, 2018, https://www.cliffordchance.com/briefings/2018/02/the_export_controlreformactof2018risksan.html; Stew Magnuson, *Export Control Reform at Risk of Reversals*, *National Defense*, March 16, 2018,

<http://www.nationaldefensemagazine.org/articles/2018/3/16/export-control-reform-at-risk-of-reversals>

¹¹⁸ Andrea Stricker with David Albright, *U.S. Export Control Reform: Impacts and Implications for Controlling the Export of Proliferation-Sensitive Goods and Technologies*, May 2017, https://isis-online.org/uploads/isis-reports/documents/Export_Control_Reform_Initiative_Review_and_Recommendations_May_2017_Final.pdf.