Defense Science Board
Task Force

On

HIGH PERFORMANCE MICROCHIP SUPPLY

February 2005

Office of the Under Secretary of Defense
For Acquisition, Technology, and Logistics
Washington, D.C. 20301-3140

AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
FEB 2005	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Report of the Defense Science Board Task Force on High Performance Microchip Supply	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Office of the Under Secretary of Defense For Acquisition, Technology, and Logistics Washington, DC 20301-3140**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**UU**	**118**	

This report is a product of the Defense Science Board (DSB).

The DSB is a federal advisory committee established to provide independent advice to the Secretary of Defense. Statements, opinions, conclusions, and recommendations in this report do not necessarily represent the official position of the Department of Defense.

This report is unclassified.

OFFICE OF THE SECRETARY OF DEFENSE
3140 DEFENSE PENTAGON
WASHINGTON, DC 20301-3140

DEFENSE SCIENCE
BOARD

MEMORANDUM FOR THE ACTING UNDER SECRETARY OF DEFENSE FOR ACQUISITION, TECHNOLOGY, AND LOGISTICS

SUBJECT: Report of the Defense Science Board Task Force on High Performance Microchip Supply

I am pleased to forward the final report of the Defense Science Board Task Force on High Performance Microchip Supply. The report makes recommendations that help ensure the long term, leading edge U.S. performance of microchip design, development, and manufacturing. The report also focuses on the future U.S. ability to ensure long term trusted and secure supplies of microelectronic components to the DOD and to the U.S. government.

The task force vision for ensuring the future of U.S. based leading edge technology and trusted supply encompasses a broad based set of recommendations and action.

The conclusion is a call for the U.S. government in general, and the DOD and its suppliers specifically, to establish a series of activities to ensure that the United States maintains reliable access to the full spectrum of microelectronics components, from commodity and legacy, to state-of-the-art parts, and application-specific Integrated Circuits special technologies. These activities must provide assurance that each component's trustworthiness (confidentiality, integrity and availability) is consistent with that component's military application.

Additionally, specific efforts to protect U.S. technical leadership and intellectual property in the microelectronics domain need to be put forth and prioritized. This includes maintenance and nurturing the U.S. electronics skill base through continuing, stable research funding.

I endorse the recommendations of the task force and encourage you to review their report.

William Schneider, Jr.
Chairman

This page intentionally left blank.

OFFICE OF THE SECRETARY OF DEFENSE
3140 DEFENSE PENTAGON
WASHINGTON, DC 20301-3140

DEFENSE SCIENCE
BOARD

MEMORANDUM TO THE CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT: Report of the Defense Science Board Task Force on High Performance Microchip Supply

It is clear from recent trends in the microelectronics industry that a significant migration of critical microelectronics manufacturing from the United States to other foreign countries has and will continue to occur. The rate of this technology migration is alarming because of the strategic significance this technology has on the U.S. economy and the ability of the United States to maintain a technological advantage in the Department of Defense (DoD), government, commercial and industrial sectors. Our greatest concern lies in microelectronics supplies for defense, national infrastructure and intelligence applications.

Our study has highlighted prior, current and projected microelectronic industry trends and proposes explanations and recommendations to address some of the current disconcerting issues.

Assured supply of trusted microelectronics components for defense systems use requires actions well beyond the scope and magnitude of those that can be mounted by a single defense supplier, or by the entire defense contractor base. Addressing this problem is a uniquely government function. DoD is charged with the defense of the United States, a mission which depends heavily on microelectronics. The task force considers DoD the logical steward to lead and foster a national solution to this critical problem, regardless of which arm of government must act. The task force also sees DoD as the logical U.S. government point to convene supplier, subsystem, prime and government users, and commercial interests, to address the recommendations in the conclusion of this report.

On a broad scale, economic and trade conditions for semiconductor manufacturers operating in the United States must be as attractive as those for manufacturers operating elsewhere. The defense department should estimate the number and varieties of microelectronic components that require trustworthiness as an aid to planning the size and scope of the Defense Trusted Integrated Circuits Strategy. Access to that design and manufacturing capability requires that the DoD purchase products and services from leading edge semiconductor firms in a way acceptable to the government, its systems contractors and to the component suppliers.

DoD needs a focused, tailored acquisition plan, driven by a long-term vision of its semiconductor needs, to establish the basis, policy and operating guidelines for DoD-enabled access to trusted foundry services by the defense department, its contractors and others. New low volume chip manufacturing models and fabrication equipment are required if future defense systems are to have unique microelectronics hardware capabilities at a reasonable cost. The same requirement for economical, modest-volume Integrated Circuits is developing for future commercial products. A reexamination of economic models for producing low-volume products will require a joint government / industry program to develop new, more flexible factory technology capable of meeting both defense and commercial needs.

The United States and its allies still maintain regimes of export controls for defense-critical and dual-use technology and equipment as one approach for limiting some technology transfers to potential adversaries. The task force recommendations address specific technologies unique to use of programmable "standard" components defense applications and assurance of component trustworthiness, DoD-unique technologies and counter-tamper proficiency.

Urgent action is recommended, as the industry is likely to continue moving in a deleterious direction resulting in significant exposure if not remedied. We urge greater than usual speed in implementing the recommendations of our study. The nation's security and economic well being demands it.



Dr. William Howard

Task Force Chairman

TABLE OF CONTENTS

EXECUTIVE SUMMARY 3
Task Force Conclusion 5
Task Force Findings and Recommendations 6
DOD Vision 7
Sizing the Problem 8
DOD Acquisition of Trusted Microelectronic Components 9
Custom IC Production Models and Technology 9
Equipment Export Controls 10
Standard chips with Programmable Hardware and/or Software 12
DOD-Unique Technologies 13
Adversarial Clandestine Operational Opportunities 14
INTRODUCTION 15
Background 16
The Threat 22
Foreign Dependence Risks 24
Defense Community Influence 25
FINDINGS 27
The Industry Situation 27
DOD Vision 32
Sizing the Problem 33
DOD Acquisition of Trusted Microelectronic Components 35
Standard and Custom Parts 39
Semiconductor Manufacturing Equipment Export Controls 42
Standard chips with Programmable Hardware and/or Software 44
DOD-Unique Technologies 48
Adversarial Clandestine Operational Opportunities 49
Conclusion 51
RECOMMENDATIONS 55
Recommendation 1 – Commit to DOD Leadership 57
Recommendation 2 – Level the Playing Field 58

Recommendation 3 – Understand the Trusted Microelectronics Need – Enumeration 62
Recommendation 4 – Develop a DOD Microelectronics Action Plan 63
Recommendation 5 – Develop Business Models, Technology, and Equipment for Economic Development and Production of Low-Volume ASICs 71
Recommendation 6 – Strengthen Bilateral and Multilateral Controls on Critical Semiconductor Manufacturing and Design Equipment 72
Recommendation 7 – Sustain Leadership in "Standard" Programmable Microchips 73
Recommendation 8 – Support DOD-Unique Technology Research and Development 75
Recommendation 9 – Enhance U.S. Countertamper Proficiency 77
APPENDIX A. TERMS OF REFERENCE 81
APPENDIX B. TASK FORCE MEMBERSHIP 83
APPENDIX C. DEPUTY SECRETARY OF DEFENSE MEMO 85
APPENDIX D. FUTURE TECHNOLOGY DEVELOPMENT 87
APPENDIX E. VERIFYING CHIPS MADE OUTSIDE THE UNITED STATES 93
APPENDIX F. TRUSTED FOUNDRY PROGRAM 95
APPENDIX G. COMPARISON OF ASIC AND FPGA SYSTEM CHARACTERISTICS 99
APPENDIX H. DFAR SUPPLEMENT 101
Defense Federal Acquisition Regulation Supplement 101
APPENDIX I. MINORITY REPORT 103
APPENDIX J. ACRONYMS 105

EXECUTIVE SUMMARY

The microelectronics industry, supplier of hardware capability that underlies much of America's modern military leadership technology, is well into a profound restructuring leading to horizontal consolidation replacing the past vertically integrated company structure. One unintended result of this otherwise sound industry change is the relocation of critical microelectronics manufacturing capabilities from the United States to countries with lower cost capital and operating environments. Trustworthiness and supply assurance for components used in critical military and infrastructure applications are casualties of this migration. Further, while not the focus of this study per se, the U.S. national technological leadership may be increasingly challenged by these changing industry dynamics; this poses long term national economic security concerns.

Accordingly, for the DOD's strategy of information superiority to remain viable, the Department requires:

- Trusted and assured supplies of integrated circuit (IC) components.
- A continued stream of exponential improvements in the processing capacity of microchips and new approaches to extracting military value from information.

Trustworthiness of custom and commercial systems that support military operations – and the advances in microchip technology underlying our information superiority – however has been jeopardized. Trustworthiness includes confidence that classified or mission critical information contained in chip designs is not compromised, reliability is not degraded or untended design elements inserted in chips as a result of design or fabrication in conditions open to adversary agents. *Trust cannot be added to integrated circuits after fabrication; electrical testing and reverse engineering cannot be relied upon to detect undesired alterations in military integrated circuits*.

Assured sources are those available to supply microelectronics components, as needed, for defense applications according to reasonable schedules and at a reasonable cost.

Pressure on U.S. IC suppliers for high return on invested capital has compelled them to outsource capital intensive manufacturing operations. Thus, the past decade has seen an accelerating trend toward vertical disaggregation in the semiconductor business. Companies whose manufacturing operations once encompassed the full range of integrated circuit activities from product definition to design and process development, to mask-making and chip fabrication, to assembly and final test and customer support, even materials and production equipment, are contracting out nearly all these essential activities.

Most leading edge wafer production facilities (foundries), with the exception so far of IBM and possibly Texas Instruments, are controlled and located outside the United States. The driving forces behind the "alienation" of foundry business from the United States to other countries include the lower cost of capital available in developing countries, through foreign nations' tax, market access requirements, subsidized infrastructure and financing incentives (including ownership), and the worldwide portability of technical skills, equipment and process know-how.

These changes are directly contrary to the best interests of the Department of Defense for non-COTS ICs. The shift from United States to foreign IC manufacture endangers the security of classified information embedded in chip designs; additionally, it opens the possibility that "Trojan horses" and other unauthorized design inclusions may appear in unclassified integrated circuits used in military applications. More subtle shifts in process parameters or layout line spacing can drastically shorten the lives of components. To the extent that COTS destinations in DOD systems can be kept anonymous, the use of COTS implies less risk. However, even use of COTS components may not offer full protection from parts compromise. Neither extensive electrical testing nor reverse engineering is capable of reliably detecting compromised microelectronics components.

A further complication in DOD's integrated circuit supply problems lies in military systems' use of microelectronic components that incorporate technologies for which there is no commercial demand. Irreducible requirements for radiation hardening, high power microwave and millimeter-wave circuits and special sensor, to name but a few, lie outside widely available commercial capabilities.

Beyond the threat of IC device compromise described above, dependence on off-shore or foreign-owned semiconductor component production subjects the United States to several risks, such as lack of quick response or surge capacity in time of war, that could threaten its access to state-of-art microelectronics. As capacity moves to potential adversary countries, the United States is vulnerable to a governmental "reverse-ITAR" by which critical technologies are denied to the U.S. in international trade.

A longer term risk lies in the historical fact that leading-edge R&D tends to follow production. The most attractive positions for talented process scientists and engineers moves with advanced production. Additionally, a separation of design from production could render the close collaboration between process engineers and designers required for leading edge chip development ineffective for U.S. defense industry.

The Defense Department does not directly acquire components at the integrated circuit level. Individual circuits are most often specified by designers of subsystems; even system primes have little knowledge of the sources of the components used in their system-level products. Any DOD acquisition plan to address IC trustworthiness and availability must focus on defense suppliers as much as DOD itself.

TASK FORCE CONCLUSION

The Department of Defense and its suppliers face a major integrated circuit supply dilemma that threatens the security and integrity of classified and sensitive circuit design information, the superiority and correct functioning of electronic systems, system

reliability, continued supply of long system-life and special technology components.

TASK FORCE FINDINGS AND RECOMMENDATIONS

Industry Situation

Finding: Semiconductor technology and manufacturing leadership is a national priority that must be maintained if the U.S. military is to continue to lead in applying electronics to support the warfighter. An integral part of that leadership is the close coupling of manufacturing with the development of advanced technology and the design of leading-edge integrated circuits. This can best be achieved if development and manufacturing are co-located.

Recommendation: To assure DOD to access leading edge trusted manufacturing facilities, the United States needs a broad national effort to offset foreign polices designed to encourage movement of leading edge semiconductor manufacturing facilities to offshore locations. A coherent U.S. policy response to counter the extensive intervention by foreign governments to encourage local investment in the semiconductor industry would include,

- U.S. government vigorous support for compliance with World Trade Organization rules.
- U.S. government steps to insure that intellectual property laws are fully enforced,
- Increased Department of Defense and intelligence agency involvement in decisions by other agencies of the U.S. government which have the potential to significantly affect the U.S. defense microelectronics industrial base,
- Increased university research funding to ensure that the U.S. remains an attractive and competitive location for the most talented students and faculty from around the world to study microelectronics,

- Continued intelligence agency monitoring of the global state of microelectronics technology to determine where additional effort is required to keep U.S. ahead of, or at least equal to, the world state of the art in critical fields, and
- Continued DOD efforts to inventory current and future trusted component needs as a basis for its long-term microelectronics acquisition plans
- The federal government needs to determine its role in assisting various States in developing their incentive packages. States should also strive to ensure that their permitting processes are responsive to business timelines.

DOD VISION

Finding: On 10 October, 2003, the Deputy Secretary Wolfowitz outlined five goals for a "Trusted Integrated Circuit Strategy:"

- Facilities Identification
- Product Identification
- Near Term Solutions
- Research Initiatives
- Healthy Commercial IC Industry

The Task Force agrees with the need for a strategy and with the elements identified in Dr. Wolfowitz's Defense Trusted Integrated Circuits Strategy (DTICS) memo.

Based on the presentations and information it has received, plus the experience of its members, the Task Force perceives that DOD has a Trusted Foundry strategy that addresses its near-term needs. However it has no overall vision of its future microelectronics components needs and how to deal with them. Technology and supply problems are addressed as they arise (e.g., radiation-hardened IC supply, sources of classified components, legacy parts). An overall vision would enable the Department to develop approaches to

meeting its needs before each individual supply source becomes an emergency, and to preempt or diffuse the threat and risks outlined above.

Recommendation: The Task Force recommends that DOD, directed by the Secretary and the Undersecretary for Acquisition, Technology and Logistics, lead in guaranteeing its needs are supported by ensuring that the United States policy and industry together transform and enhance the U.S. position in onshore microelectronics. Providing for assured supplies by DOD contracts with today's trusted foundries helps solve the immediate problem, but is only a temporary measure; foundry agreements will not address the structural issue of funding research that will sustain our information superiority. Long term national security depends upon U.S.-based competitiveness in research, development, design and manufacturing. DOD should advocate that these are not only DOD objectives but also national priorities.

SIZING THE PROBLEM

Finding: The Task Force attempted to estimate DOD's IC requirements to size the problem facing future U.S. military integrated circuits acquisition needs. A precise evaluation of DOD's IC consumption is not possible; a rough estimate is 1-2% - a small fraction of global demand. Based on data it has gathered, the Task Force estimates that at least 50-60 new critical part types are being generated per year within DOD – a number that is likely to increase over the next several years as signal processing becomes more distributed.

Although DOD-unique IC consumption is a small fraction of the commercial market, the functions performed by these special circuits are essential to the nation's defense.

Recommendation: DOD must determine classes of ICs incorporated in its weapon systems and other key mission products that require trusted sources and how many such circuits are needed. This requires that DOD identify device and technology types of microelectronics devices that require trusted sources as well as the

length of time it will need such special supply arrangements. This identification must include the full range of technologies needed for DOD as well as its suppliers.

DOD ACQUISITION OF TRUSTED MICROELECTRONIC COMPONENTS

Finding: Throughout the past ten years, the need for classified devices has been satisfied primarily through the use of government-owned, government- or contractor-operated or dedicated facilities such as those operated by NSA and Sandia. The rapid evolution of technology has made the NSA facility obsolete or otherwise inadequate to perform this mission; the cost of continuously keeping it near to the state of the art is regarded as prohibitive. Sandia is not well suited to supply the variety and volume of DOD special circuits. There is no longer a diverse base of U.S. IC fabricators capable of meeting trusted and classified chip needs.

DOD has initiated a Trusted Foundry Program to provide, in the interim, a source of high performance ICs in accordance with the overall DTICS mandate. DOD has contracted for these services on a "take-or-pay" basis. This program is a good start addressing immediate needs for trusted sources of IC supply, however a more comprehensive program is needed that looks further into the future.

Recommendation: Led by the USD(AT&L), DOD and its Military Departments/Agencies, working with their system suppliers, must develop a plan of action that encompasses both short- and long-term technology, acquisition and manufacturing capabilities needed to assure on-going availability of supplies of trusted microelectronic components. This plan of action requires both a steady-state vision and implementation plans for both standard and special technology components.

CUSTOM IC PRODUCTION MODELS AND TECHNOLOGY

Finding: Commercial integrated circuit production methods and production technology has become strongly skewed to

manufacturing commodity products. Costs of high volume standard products have continued to fall, however this mass production trend has dramatically raised the cost of low production volume leading-edge custom products beyond affordability.

Since military systems very often require a few parts with unique functions, state-of-the-art speed and low power, DOD and its suppliers have an irreducible need for custom components. A similar need is arising in industry. The solution to this quandary lies in development of a new model for economic production of limited volume custom circuits and equipment.

Developing cost-effective technology for the design and fabrication of low production volume, leading edge technology ASICs will require the combined efforts of DOD, the semiconductor industry and semiconductor fabrication equipment suppliers.

DARPA attempted such a development in the mid-1990s through its MMST program; however that program had different goals than those required today.

Recommendation: DDR&E should take another look at ASIC production and formulate a program to address barriers to low- to medium-volume custom IC production. This program will require a dedicated, joint effort by all participants in ASIC production - designers, fabricators and equipment makers. Such an effort could be similar to SEMATECH, the industry-initiated, DARPA supported consortium.

EQUIPMENT EXPORT CONTROLS

Finding: Dual use technology exports which pose national security or foreign policy concern are regulated pursuant to the Export Administration Act of 1979. Advanced semiconductor manufacturing equipment and technology are regarded as sensitive, and export to destination such as China requires issuance of an export license by the Department of Commerce (DoC). Applications for export licenses are reviewed by DoC as well as the Department of Defense and the State Department. Decisions to grant or not grant

licenses are determined on a case-by-case basis. Since the end of the Cold War U.S. export controls have become less effective in restricting the flow of advanced semiconductor manufacturing equipment (SME) and design technology and equipment to China.

The strict international regime of export controls that governed semiconductor design and production equipment exports during the Cold War, CoCom, was replaced in 1996 by the less rigorous Wassenaar Arrangement, a non-treaty, voluntary system for coordinating and sharing information with respect to the export of sensitive technologies. On several occasions, the U.S. government has sought to persuade other Wassenaar members to restrict exports of SME to China, but has been rebuffed.

Recommendation: The Wassenaar Arrangement covering exports of sensitive, leading edge semiconductor manufacturing equipment (SME) is not an effective tool for assuring that potential adversaries do not have access to leading edge design and wafer fabrication equipment, technology and cell libraries. The U.S. should act to strengthen export controls by:

- Negotiating bilateral agreements or understandings with Wassenaar members in which advanced SME and design tools are made with the objective of harmonizing export licensing practices and standards,
- Concluding a similar bilateral agreement or understanding with Taiwan.
- Giving the Department of Commerce a mandate and resources to compile an up-to-date catalogue of the global availability (including foreign availability) of state-of-the-art SME and design tools in designated foreign countries.

STANDARD CHIPS WITH PROGRAMMABLE HARDWARE AND/OR SOFTWARE

Finding: Defense system electronic hardware, like that used in commercial applications, has undergone a radical transformation. Whereas custom circuits, unique to specific applications, were once widely used, most information processing today is performed by combinations of memory chips (DRAMs, SRAMs, etc.) which store data (including programs), and programmable microchips, such as Structured ASICs, Programmable Logic Arrays (PLAs), central processors (CPUs) and digital signal processors (DSPs), which operate on the data. Of the two classes of parts, the latter have more intricate designs, which make them difficult to validate (especially after manufacturing) and thus more subject to undetected compromise.

U.S. companies have led in design of programmable microchips since their inception. Although U.S. design leadership does not in and of itself assure the trustworthiness of these parts, it does put the DOD in a superior position to potential adversaries, whose systems rely on U.S. based suppliers and/or inferior parts procured abroad. This advantage accrues not only to fielded weapon systems, but to all aspects of the defense community and of U.S. national infrastructures.

U.S. leadership cannot be taken for granted, especially in light of the global dispersion underway in the semiconductor industry.

Recommendation: Continued development of new programmable technologies is key to sustaining U.S. leadership. To support these developments, DOD should:

- Partner with industry and with other government agencies, especially the NSF and Homeland Security, to fund university research that will ensure the domestic supply of scientists and engineers who are skilled in the development and use of programmable hardware,

- Should foster the voluntary exchange of best counter-tampering practices for assuring trust of standard programmable hardware among government and U.S. commercial semiconductor developers, through the creation of courseware and industry information exchange programs,
- Institute a targeted program in the area of firmware integrity to rapidly develop, disseminate and encourage adoption of improvements to this trust-related aspect of programmable parts, and in conjunction with the above, initiate a research program on "design for trust evaluation" along the lines of prior successful efforts on "design for testability."

DOD-UNIQUE TECHNOLOGIES

Finding: Defense systems, by the nature of their functions and use environment, require some technologies for which there is no wide commercial demand. The most widely known of these "special" technologies is that of radiation-hardening of circuits to allow their operation / survival through a nuclear event. Similar unique technologies include low power and counter-tamper techniques. Research and development for these special technologies is supported, almost entirely, by DOD through DTRA, NSA or similar mission agencies.

Recommendation: DOD must continue to support research and development of the special technologies it requires. This includes on-going radiation hardened and EMP-resistant component design and process development. The emergence of requirements for trustworthiness requires new efforts in technologies to embed, assure and protect component trust. The Department will require additional technology development efforts, including:

- Reducing barriers to radiation-tolerant "standard" designs,

- Increasing efforts to develop tamper protection technology, and
- Developing design and production techniques for disguising the true function of ICs.

ADVERSARIAL CLANDESTINE OPERATIONAL OPPORTUNITIES

Finding: Because of the U.S. military dependence on advanced technologies whose fabrication is progressively more offshore, opportunities for adversaries to clandestinely manipulate technology used in U.S. critical microelectronics applications are enormous and increasing. In general, a sophisticated, clandestine services develop opportunities to gain close access to a target technology throughout its lifetime, not just at inception.

If real and potential adversaries' ability to subvert U.S. microelectronics components is not reversed or technically mitigated, our adversaries will gain enormous asymmetric advantages that could possibly put U.S. force projection at risk. In the end, the U.S. strategy must be one of risk management, not risk avoidance. Even if risk avoidance were possible, it would be prohibitively costly.

Recommendation: Accurate characterization and assessment of adversaries' "dirty tricks" is essential to develop an effective U.S. counter tamper strategy. The Task Force addressed many of these issues relative to the security challenges of information sharing, but opportunities, methods and threats change continuously. The DDR&E in conjunction with the Intelligence Community should develop risk mitigating technical approaches to support the risk management function. DDR&E should take the lead in defining the requirements and making the necessary investments to realize the needed security breakthroughs

INTRODUCTION

The microelectronics industry, supplier of hardware capability that underlies much of America's modern military leadership technology, is well into a profound restructuring leading to horizontal consolidation replacing the past vertically integrated company structure. This restructuring is driven by the need to spread large and rapidly increasing capital risks widely, across a broad industry base. One unintended result of this otherwise sound industry change is the relocation of critical microelectronics manufacturing capabilities from the United States to countries with lower-cost capital and operating environments. From a U.S. national security view, the potential effects of this restructuring are so perverse and far reaching and have such opportunities for mischief that, had the United States not significantly contributed to this migration, it would have been considered a major triumph of an adversary nation's strategy to undermine U.S. military capabilities. Trustworthiness and supply assurance for components used in critical military and infrastructure applications are the casualties of this migration. Further, while not the focus of this study per se, the U.S. national technological leadership may be increasingly challenged by these changing industry dynamics; this possibility poses long-term national economic security concerns.

Although this study focuses on microelectronics components, changes underway in the semiconductor industry may apply to other critical military electronics technologies: circuit boards, subsystems assemblies, and, especially, software. DOD cannot and should not disengage from its allies and from seeking supply from the global marketplace, but defense systems and other mission-critical products designed and procured abroad need appropriate oversight and controls to ensure trustworthiness.

The superiority of U.S. forces depends on information superiority, which rests on having superior sensors and superior information processing and networking capabilities. These capabilities, in turn,

depend on sustained improvements in the performance of microchips (see appendix D).[1]

Accordingly, for the DOD's strategy of information superiority to remain viable, the department requires:

- Trusted[2] and assured[3] supplies of integrated circuit (IC)[4] components.
- A continued stream of exponential improvements in the processing capacity of microchips and new approaches to extracting military value from information.

BACKGROUND

It is now taken for granted that microelectronics-based weapons, communications, navigation, space, sensor, intelligence, and battle management systems provide the force multipliers that made the

1. Improvements in sensors are typically linear, i.e., the fidelity of individual sensors increases linearly with time. However, the "take" of raw information increases exponentially owing to complementary growth in the diversity and number of sensors available. This, in turn, drives exponential growth in the demand for information processing and network capacity. The demand for processing power is also driven by the simple observation that for every "n" bits of information that are acquired, there are 2^n permutations, only a fraction of which will be of interest. Although exhaustive examination of all of those permutations would be intractable, the DOD has to date excelled at combining exponential growth in the processing capacity of individual microchips with improvements in the sophistication of the algorithms that are used to wring "signals" from data. Note that information superiority does not simply accrue from the use of microchips in large supercomputers but depends on the processing performance of microchips that are embedded within a wide range of DOD systems, both large and small.
2. "Trusted" ICs and microelectronic components, in the context of this study, are those that can be employed by a user with confidence that they will perform as expected and are free from compromises, denials or exploitation.
3. "Assured" supplies are manufacturing capabilities that are available to produce needed quantities of microelectronics components throughout the life of their system applications.
4. Integrated Circuits (ICs) are microelectronic components that combine multiple circuit elements on a single semiconductor chip. ICs dominate today's electronic systems, performing often complex, high-performance, reliable analog, digital and RF functions.

revolution in military affairs possible. The hardware underlying these systems incorporates many classified capabilities, accounts for reliability, uses special technologies, and enables the long lives of today's military systems. Trusted and assured supplies of integrated circuit components for military applications are critical matters for U.S. national security, yet the defense fraction of the total integrated circuits market is minuscule (1 or 2% now versus 7% in the 1970s)[5]; supplier strategies are driven entirely by economic and market pressures affecting company health and competitiveness.

In response to the increasing commercial availability of high-performance ICs, U.S. defense acquisition has emphasized use of commercial off-the-shelf (COTS) components in new system designs. Further, the military specifications (MIL-SPEC) system that drove 1970s defense hardware acquisitions was left behind, often in favor of commercial performance and reliability specifications. Substantial benefits have followed as a consequence of these acquisition decisions – cost, performance, and development times of microelectronic elements of defense systems have improved markedly[6].

Trustworthiness of custom and commercial systems that support military operations – and the advances in microchip technology underlying our information superiority – have been jeopardized[7]. Trustworthiness includes confidence that classified or mission-critical information contained in chip designs is not compromised, reliability is not degraded, and unintended design elements are not inserted in chips as a result of design or fabrication in conditions open to adversary agents. **Trust cannot be added to integrated circuits after fabrication; electrical testing and reverse engineering cannot be relied upon to detect undesired alterations in military integrated circuits.[8]** While not wholly sufficient -- circuit boards, subassemblies,

5. Military share reference. See: "Sizing the Problem" in the findings section
6. Special Technology Review on Commercial Off-the-Shelf Electronic Components, DOD Advisory Group on Electron Devices, June 1999.
7. Ray Price, Briefing to the Defense Science Board Task Force on High-Performance Microchips Supply, May 20, 2004.
8. Randy Goodall, SEMATECH Director, External Programs: Briefing to the Defense Science Board Task Force on High-performance Microchip Supply, June 23, 2004 see Appendix E.

and software may also pose concerns -- trusted electronic components are key and necessary elements to guarantee performance of defense systems, but are not sufficient.

Assured sources are those available to supply microelectronics components as needed for defense applications according to reasonable schedules and at a reasonable cost. Changes in the semiconductor industry structure also jeopardize DOD's ability to procure needed microelectronic components in emergencies and throughout the long lives of military systems.

The past decade has seen an accelerating trend toward vertical disaggregation in the semiconductor business.[9] [10] [11] Companies whose manufacturing operations once encompassed the full range of integrated circuit activities from product definition to design and process development, through mask-making and chip fabrication, through assembly and final test and customer support, and even including materials and production equipment, are outsourcing nearly all these essential activities. Materials and production equipment supply developed into separate industries 20 years ago. Company rationale for this divestiture was sound: firms that perform capital-intensive activities for many customers divide their fixed costs among them all. Further, the need for these firms to compete in the open market distills the best supply sources. Next came external mask-fabrication for lithography. Recent trends point to company outsourcing of virtually all manufacturing operations, including chip fabrication, assembly, and testing as well as process development.

9. Daryl Hatano, SIA: *Fab America –Keeping U.S. Leadership in Semiconductor Technology*, Presentation to the Defense Science Board Task Force on High-Performance Microchips, March 3, 2004.
10. Firms that specify and design integrated circuits which are then produced under contract foundries and assembled and tested by contractors are called "fabless." Fabless IC companies exhibit better financial performance than vertically integrated firms because of their low capital investment, greater flexibility and need for less process engineering. They are increasingly being emulated by historically vertically integrated manufacturers (sometimes called Integrated Device Manufacturers, or IDMs).
11. Bob Stow and George Nossaman (BAE Systems): *Rad Hard Microelectronics Supply* Presentation to the Defense Science Board Task Force on High-Performance Microchips, March 3, 2004.

Design and development will soon follow. Fabless IC production has grown to 16% of the total industry (see Figure 1); the fraction fabless production at the leading technology edge is much higher. The prototypical integrated circuits supplier in 10 years is likely to specify products that will then be designed, manufactured, assembled, and tested by contractors and sold through outside representatives and distributors. Historical vertical integration in the semiconductor industry has been replaced by horizontal consolidation of chip fabrication, mask making, material supply, assembly, testing, and equipment supply. This consolidation has led to global dispersion of manufacturing operations, removing many critical operations from U.S. national control.

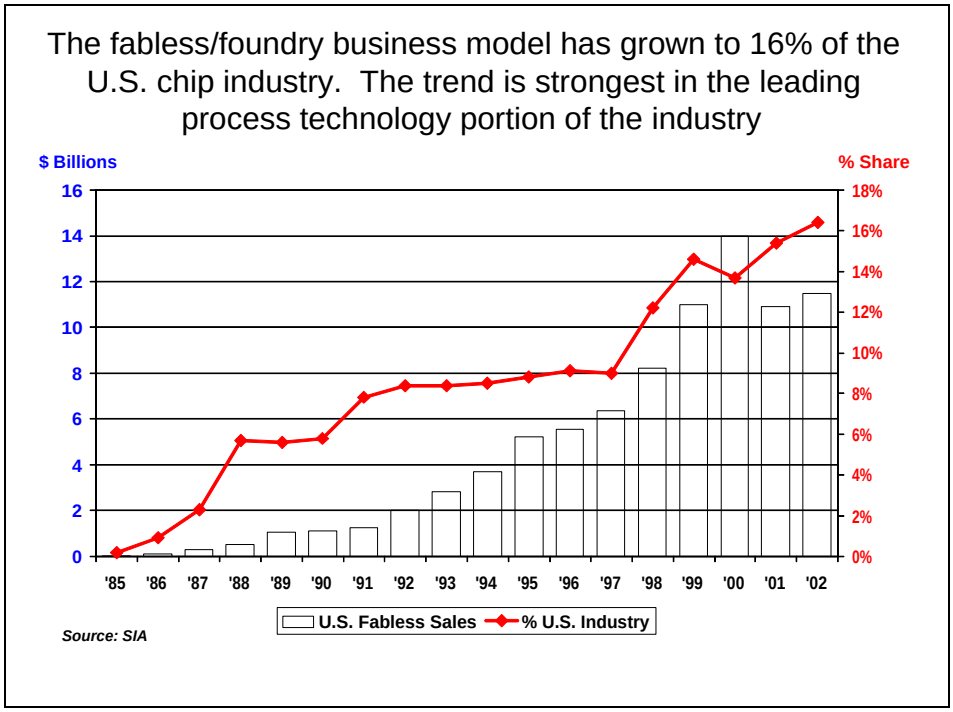


Figure 1

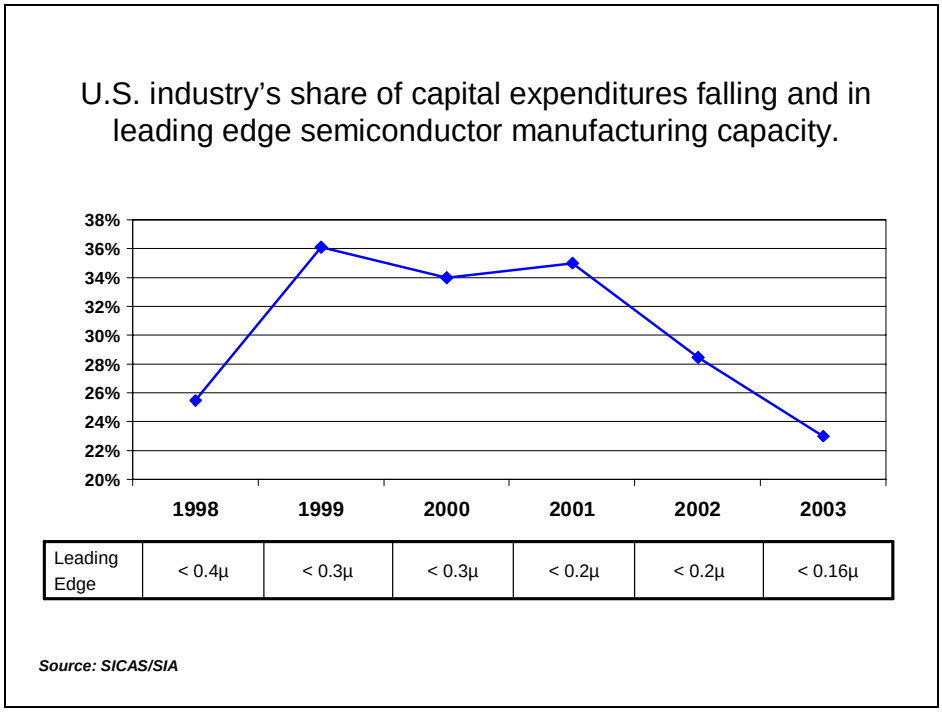


Figure 2

The hollowing out of previously vertically integrated companies into fabless firms is the direct result of the rapid technology progress that characterizes the integrated circuits industry. As technology has surged forward, the cost of building factories has risen dramatically (now approaching three billion dollars for a full-scale, 300 mm wafer, 65 nm process chip fabrication plant). Irresistible pressures for economies of scale, huge nonrecurring product development expenses, and the need for sophisticated design and test techniques have forced consolidation of leading-edge product realization functions into huge, specialized wafer processing facilities, referred to

as "foundries," [12] which offer unique services to the broad industry customer base. Foundries spread the huge costs (both skills and money) across multiple customers, thereby attaining economies of scale not possible in a single company's operations. Contract assembly started in the 1970s. Wafer fabrication foundries that accept business from all qualified customers are a relatively new development in the semiconductor business; they arose in the 1990s to serve the needs of a new breed of chip companies who lacked in-house manufacturing capability. The impressive financial performance of these industry latecomers has put pressure on traditional chip firms to follow suit, to become "fab-light." As a result, after rising to 35% in 1999 to 2004, the U.S. semiconductor industry fraction of world-wide semiconductor capitol investment in leading edge technology has fallen to 20% (see Figure 2)

Strategic decisions by several countries that indigenous leading-edge integrated circuits capability is key to their economic future has aided and abetted movement of U.S. IC manufacturing and development abroad. These countries implement their strategies through a wide variety of economic incentives and support.

Most leading-edge wafer foundries (with the exception so far of IBM and possibly Texas Instruments) are controlled and located outside the United States. Although cost of labor was the initial consideration driving integrated circuit manufacturing off-shore, automation and inflation has now erased much of this advantage. Nevertheless, virtually all integrated circuit assembly and most integrated circuit testing is performed abroad, where the greatest competence for these activities now resides.

Today the driving force behind the "alienation" of foundry business from the United States to other countries is the lower cost of capital available in developing countries, made possible by foreign nations' tax incentives, market access requirements, subsidized infrastructure, and low-cost financing (including ownership), in combination with the worldwide portability of technical skills,

12. A "foundry," for purposes of this study, is a wafer production facility that fabricates IC designs for a broad customer clientele as a major part of its business.

equipment and process know-how. Sophisticated process knowledge is now provided by equipment suppliers as part of equipment purchases. Scientists and engineers trained in U.S. graduate schools are free to move to other nations. In some cases, students may no longer seek education in the United States; for example, the number of engineering graduates in China is far outpacing U.S. totals so that students no longer have to come to the U.S. to attend school. The primary beneficiary countries of the foundry trend have been in the Far East (Taiwan, Singapore, People's Republic of China, Korea, and Japan), some of whose future interests may not align with those of the United States. Taiwan dominates global foundry production with about two-thirds of current capacity; China, a relatively new entrant with 8 percent of global capacity, is rapidly increasing its market share.

Similar trends are evident in the mask-making and materials businesses that support integrated circuit fabrication. These ancillary industries, like that of integrated circuit fabrication, play critical roles in the integrity of the military microelectronic components supply.

THE THREAT

The changes underway in the integrated circuit supply structure are directly contrary to the best interests of the Department of Defense with regard to non-COTS ICs. The shift from United States to foreign IC manufacture endangers the security of classified information embedded in chip designs; additionally, it opens the possibility that "Trojan horses" and other unauthorized design inclusions may appear in unclassified integrated circuits used in military applications. These surreptitious inclusions are similar to viruses, Trojan Horses, and worms[13] common in today's public

13. A **Trojan horse** is a program that disguises itself as another program. Similar to viruses, these programs are hidden and usually cause an unwanted effect, such as installing a back door in your system that can be used by hackers. **Worms** spread without any user interaction, typically by exploiting a flaw in popular software. Once activated, they generally use the Internet or your LAN (local network) to self-propagate and often take advantage of vulnerabilities in email programs.

software networks. Such backdoor features could be used by an adversary to disrupt military systems at critical times. More subtle shifts in process parameters or layout line spacing can drastically shorten the lives of components. To the extent that COTS destinations in DOD systems can be kept anonymous, the use of COTS implies less risk. However, even use of COTS components may not offer full protection from parts compromise. Neither extensive electrical testing nor reverse engineering is capable of reliably detecting compromised microelectronics components.

The increasing complexity and sophistication of microelectronics design and fabrication technology presents additional integrated circuit supply difficulties. Advances in integrated circuits manufacturing technology make possible increasingly smaller critical dimensions of individual devices that comprise a chip's circuits. These critical dimensions are now approaching 50 nanometers (fifty billionths of a meter or 2 microinches). Lithography tools and materials necessary to perfectly define patterns with dimensions much smaller than the wavelength of visible light have become prohibitively expensive for any but the highest-manufacturing-volume products. Further, the sophisticated deposition and etch processes required to create such tiny switches are economically feasible only on huge 300mm-diameter wafers.

In IC design and manufacturing, the emphasis is on economies of scale. The commercial market has moved away from complex, low-cost, low-production-volume products because of their high costs. The combination of high nonrecurring lithography costs and large wafer size make leading edge integrated circuit products with lifetime requirements for few parts, such as those used in military systems, uneconomical. While today's high-volume fabrication emphasis is on 300 mm wafers, the need to convert to 450 mm wafers is forecast by industry in order to meet the historic cost-per-gate trend that drives IC industry economics.

To further complicate DOD's integrated circuit problems, military systems use many microelectronic components that must incorporate technologies for which there is no commercial demand. Irreducible requirements for radiation hardening, high-power microwave, and

millimeter-wave circuits and special sensor requirements, to name but a few, lie outside widely available commercial industrial capabilities.[14]

FOREIGN DEPENDENCE RISKS

Beyond the threat of IC device compromise described above, dependence on off-shore or foreign-owned semiconductor components subjects the United States to the risk that several circumstances, such as quick response or surge capacity in time of war, could threaten its access to state-of-the-art microelectronics. Some of these risks are a result of the concentration of the foundry industry into a few Far Eastern countries.

Political/Geographic Dislocations

In September 1999, an earthquake measuring 7.6 on the Richter scale hit Taiwan, shutting down all factories in Hsinchu, the national wafer fabrication center. Fortunately, these plants were restarted in a matter of weeks; however, a temblor that seriously damaged Taiwan's wafer capacity would have started a worldwide run on commercial wafer capacity that would have taken years to rectify. During such a time, DOD and its contractors would have little leverage to obtain needed fabrication services.

A major armed confrontation between Taiwan and China over the Straits of Taiwan would have similar consequences.

As additional capacity moves to potential adversary countries, the United States is vulnerable to a governmental "reverse-ITAR"[15] by which critical technologies are denied to the United States in international trade. In the late 1980s, the Japanese denied leading-edge semiconductor manufacturing tools to U.S. manufacturers, resulting in the need for SEMATECH, a rush joint effort by DARPA

14. Critical Assessment of Technologies, DOD Advisory Group on Electron Devices, 2002.
15. International Traffic in Arms Regulations (ITAR) is the set of procedures used by the United States to restrict international shipment of arms and defense-related technology.

and industry to rebuild U.S. equipment base. Denial of advanced foundry services could be much more difficult to counter.

Loss of U.S. National Technological Leadership

Delays in making leading-edge technology available to U.S. firms (as happened in the 1980s with Japanese advanced lithography tools) slow the time to market for U.S. advanced systems. Loss of leadership in critical advanced microelectronics technologies would slow the entire commercial and defense product development process.

One way such a loss could occur lies in the historical fact that leading-edge research and development (R&D) tends to migrate to production leaders. The most attractive positions for talented process scientists and engineers move toward advanced production. The close collaboration between process engineers and designers required for leading-edge chip development could be rendered ineffective for the U.S. defense industry.

DEFENSE COMMUNITY INFLUENCE

The Department of Defense and its contractors can do little on their own to ameliorate the department's integrated circuit supply problems by influencing the way the industry as a whole acts. The economic forces that drive the industry restructuring are too strong, and the military share of the integrated circuits business is at least an order of magnitude too small. The U.S. IC industry, as a whole, is relatively healthy financially and still holds the technological edge, at least for now; maintenance of its military segment, however, has a dismal future as it is now headed. Satisfying DOD unique requirements will require special attention, especially at the leading edge of process technology.

The changes in integrated circuit supply capability and the cost of leading-edge, complex ASICs[16] has discouraged DOD use of unique,

16. An ASIC, or Application Specific Integrated Circuit, is a custom IC designed for a single, application.

special-purpose integrated circuits in new systems. Instead, subsystems designers are looking for solutions that employ older chip technologies or have moved to field programmable gate arrays (FPGAs) at the sacrifice of circuit speed and increased power.

A further complication lies in the fact that the Defense Department does not directly acquire components at the integrated circuit level. Individual circuits are most often specified by the designers of subsystems; even system primes have little knowledge of the sources of the components used in their system-level products. Any DOD acquisition plan to address IC trustworthiness and availability must focus on defense suppliers as much as DOD itself.

FINDINGS

THE INDUSTRY SITUATION

Semiconductor technology and manufacturing leadership is a national priority that must be maintained if the U.S. military is to continue to lead in the application of electronics to support the warfighter. An integral part of that leadership is the close coupling of manufacturing with the development of advanced technology and the design of leading-edge integrated circuits. This coupling can best be achieved if development and manufacturing are colocated. Doing so provides an advantage to integrated device manufacturers who are able to coordinate design and process development to be first to market with leading-edge products. The transfer of technology from the laboratory to manufacturing is facilitated.

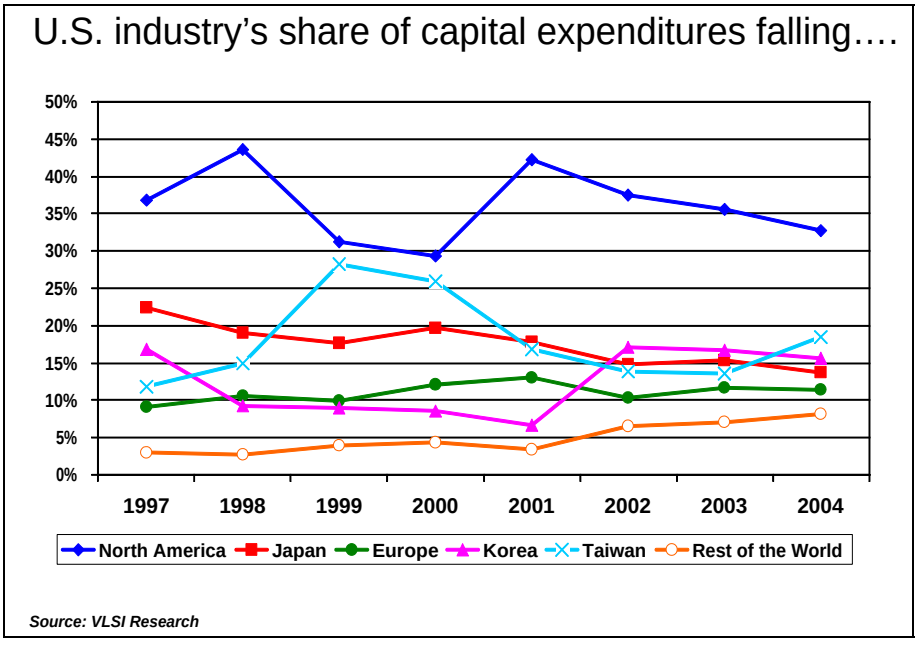


Figure 3

There is ample evidence that capital investment in the semiconductor industry is moving offshore (see Figure 3). The U.S. industry's share of capital expenditures has decreased from a high of 42% of the world's total investment in 2001 to 33% projected for 2004.[17]

By the end of 2005, there will be 59 300-mm fabrication plants (fabs) worldwide with only 16 of these located in the United States (see Figure 4). As measured by capacity, this will be the first time that less than 25% of advanced capacity is located in the United States.[18]

Of the 16 U.S. advanced technology fabrication facilities, most are special-purpose memory or microprocessor plants, adapted to a single product type and not suitable to meet government ASIC needs. Only one for sure and at most possibly three of the U.S.-based production fabs are accessible for the DOD to produce trusted microelectronics (one is currently under contract).

17. Daryl Hatano: *Fab America –Keeping U.S. Leadership in Semiconductor Technology*, Presentation to the Defense Science Board Task Force on High Performance Microchip Supply, March 3, 2004.
18. Ibid.

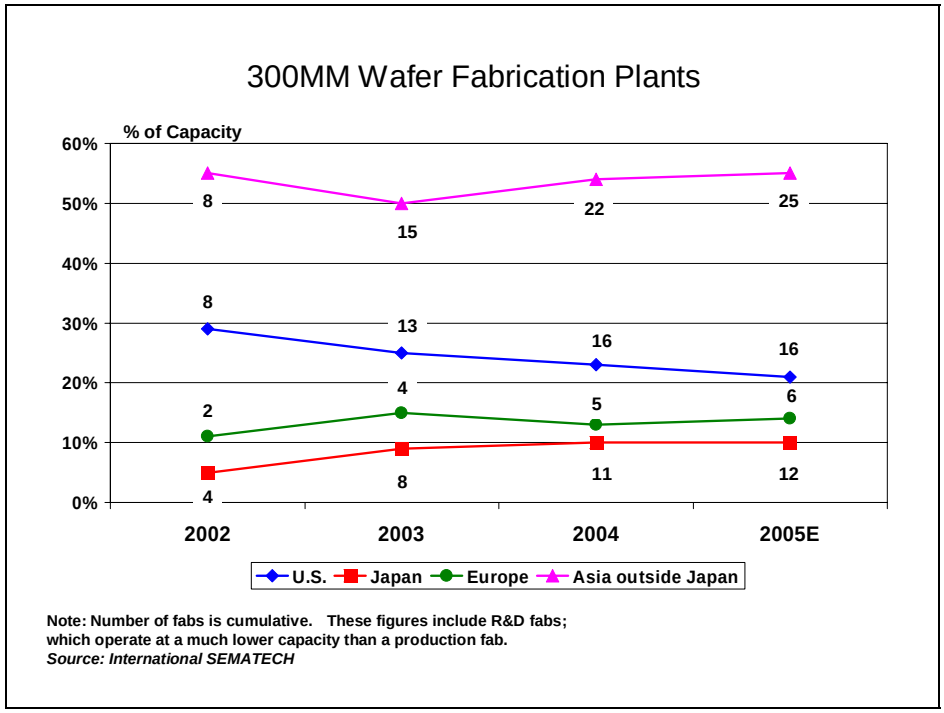


Figure 4

This movement is the result of market forces, business models, and human resource trends. Government policies also affect the location of manufacturing and technology. These policies are guided by goals such as those of China:

> With 5 to 10 years' effort….domestic integrated-circuit products will also satisfy most domestic demand and be exported as well while reducing the development and production gap with developed countries.
>
> *China State Council Document Number 18*
> *June 24, 2000*

The initial impetus (in the 1960s and 1970s) for U.S. firms to manufacture abroad was lower labor cost for IC assembly and packaging. Before extensive automation of virtually all phases of the manufacturing process, labor was an important element in product cost. The driving force behind manufacturing abroad has now

changed: a Semiconductor Industry Association document, *China's Emerging Semiconductor Industry* (October 2003), concluded

> There is almost no cost difference between locating a facility in the United States, Taiwan, or China with respect of building and equipping…Manufacturing costs [in China] are [only] 10% lower than in the United States while manufacturing cost in Taiwan are 7% lower. Almost all…accounted for by labor costs.
>
> This data… does not support the hypothesis that the concentration of new foundry investment in Taiwan and the current migration to China is due to lower construction and operating costs…Government policies are driving this…
>
> The true challenge posed by China's promotion effort to the United States and U.S. semiconductor industry is that China's growing "gravitational pull" will draw capital, talented people and ultimately, leading edge R & D and design functions away from the U.S . . . should this occur, the United States would confront the erosion of the basic institutional and human infrastructure necessary to sustain world leadership in [nano] electronics . . ..

China has adopted aggressive policies to promote domestic manufacture of semiconductors. Income tax incentives include a five year tax holiday plus five years at half-tax for reinvested capital with the clock starting when profits start. It is providing free land for industrial parks. Until recently, China applied a 17% value-added tax (VAT) to imported chips, but not to those made in China. Agreements with the World Trade Organization on VAT may have negated the impact of the full 17% on imported chips however while amounts over 3-6% are still rebated for Chinese-made chips.

Taiwan has adopted policies to encourage Taiwanese companies to keep "roots in Taiwan." A "Statute for Upgrading Industries" allow authorities to support targeted industries. Taiwan's tax law provides five-year tax holidays for semiconductors. (Taiwan's major semiconductor companies have paid little taxes for years.) To help finance the significant costs required to build chip facilities or start up microelectronics-related companies, Taiwan has a number of

government subsidy funds and government-controlled banks. Further, the personal income tax laws allow employees at high-tech firms to receive stock as compensation virtually tax free. This policy enables Taiwanese companies to compete effectively for engineering talent in the worldwide market. It is effective in attracting new advanced-degree graduates from top U.S. universities to return to Taiwan.

The SIA 2003 China report concludes:

> No U.S. policy exists with respect to the largely tax-free environment for semiconductor manufacturing and design firms in China/Taiwan. China is replicating Taiwanese policies which virtually exempt semiconductor firms from payment of corporate income tax. Such tax rules were a primary factor underlying massive semiconductor investments in Taiwan in the 1990s and are now being implemented in China . . . differences in national tax policies are becoming an important factor underlying location decisions in the semiconductor industry, and absent a U.S. policy response, such differences will increasingly determine where semiconductors are designed and produced.

Japan has also promoted semiconductor production by allowing up to 88% depreciation of production equipment in the first year. The United States allows 20%.

The Korean government has a history of supporting the semiconductor industry stretching back to the Korean government-sponsored Korean Institute of Electronics Technology (KIET), which jump-started the industry in the 1980s. They have provided capital to a private company, Hynix, through government-controlled banks because it considers semiconductors to be a backbone industry that cannot be allowed to fail from market pressures. The capital flows have included debt forgiveness, extensions of maturities, and debt-for-equity swaps.

Asian countries are not alone in using economic subsidies to attract new fabrication facilities of United States–based semiconductor companies. In February 2004, Advanced Micro

Devices, Inc. (AMD) welcomed the European Union (EU) Commission's approval of investment aid for its next-generation microprocessor wafer facility, AMD Fab 36, in Dresden, Germany. The Federal Republic of Germany and the Free State of Saxony are providing investment allowances and investment grants of up to approximately $545 million — the highest benefit possible under the German grants and subsidy program. Hiring for AMD Fab 36 is underway, and headcount for the new fab is planned to reach approximately one thousand by 2007. AMD expects to invest approximately $2.5 billion through 2007 in AMD Fab 36. Construction of a new, dedicated 24-megawatt energy center has also begun adjacent to the AMD fab.[19]

DOD VISION

On October 10, 2003, Deputy Secretary of Defense Wolfowitz outlined five goals for a "Trusted Integrated Circuit Strategy":[20]

- Facilities identification
- Product identification
- Near-term solutions
- Research initiatives
- Healthy commercial IC industry

The task force agrees with the need for a strategy and with the elements identified in Dr. Wolfowitz's Defense Trusted Integrated Circuits Strategy (DTICS) memo.

Based on the presentations and information it has received, plus the experience of its members, the task force perceives that DOD has a trusted foundry strategy that addresses its near-term needs. However it has no overall vision of its future microelectronics components needs and how to deal with them. Technology and

19. See Advanced Micro Devices, Inc. Web site: http://www.amd.com/us-en/Corporate/VirtualPressRoom/0,,51_104_543%7E79105,00.html.
20. Memo from the Deputy Secretary of Defense, "Defense Trusted Integrated Circuits Strategy", dated October 10, 2003, Ref. U16619/03 - see Appendix C.

supply problems are addressed as they arise (e.g., radiation-hardened IC supply, sources of classified components, legacy parts). An overall vision would enable the department to develop approaches to meeting its needs before each individual supply source becomes an emergency, and to preempt or diffuse the threats and risks outlined above. The needs addressed should include life-cycle and logistics needs for microelectronic components.

SIZING THE PROBLEM

The task force has attempted to estimate DOD's IC requirements to size the problem facing future U.S. military integrated circuits acquisition needs. An initial step DOD must take is to identify and characterize the volume and scope of microelectronics that require trusted sources.

Several features characterize DOD microelectronics demand today

DOD demand volume is a small fraction of global IC market demand. Based on a top-down estimating technique developed by the Institute for Defense Analysis for the deputy under secretary of defense for industrial policy DUSD(IP), the total DOD-related demand for semiconductors may be upwards of $3.6 billion in fiscal year 2004.[21] This very rough estimate is broadly defined and should be considered as including DOD's use of ICs that are incorporated in commercial or modified commercial products that it purchases, such as personal computers. The Semiconductor Industry Association website[22] estimates the expected total global sales for semiconductors in 2004 to be $214 billion. Comparing these two estimates, the DOD's share of global demand is between 1–2%.

Using the $3.6 billion a year estimate as a starting point, IDA has estimated DOD ASIC demand to be roughly $300–400 million a year. This estimate is very crude, and it likely overstates DOD's needs. It is

21. Reference to IDA study.
22. See Semiconductor Industry Association website: http://www.sia-online.org/downloads/ACFE8.pdf.

based on the EIA estimate that ASICS worldwide represent about 9% of all semiconductors and likely overstates DOD's needs. The task force understands that IDA is working for DUSD(IP) to develop a more complete and representative top-down estimating technique for DOD ASIC use. Meaningful estimates of DOD IC consumption are difficult to assemble: items like nonrecurring costs associated with IC development may or may not be included with production costs. DOD should be prepared to accept that an accurate estimate will be very difficult to make.

Although DOD-unique IC consumption is a small fraction of the commercial market, the functions performed by these special circuits are essential to the nation's defense. Electronics included in GPS systems, special intelligence equipment, M1A1 gun sights, advanced digital communications equipment (e.g., JTRS), radar electronically steerable arrays and signal processing, Synthetic Aperture Radar (SAR), communications protection devices (e.g., cryptography), and remotely piloted vehicles all use embedded ASICs. Unique low-power technologies are particularly important in DOD portable applications.

Because many DOD ASICs are designed by contractors and their suppliers, an accurate count of current and future needs is nearly impossible. Based on data it has gathered, the task force estimates that at least 50–60 new critical part types are being generated per year within DOD – a number that is likely to increase over the next several years as signal processing becomes more distributed. An estimate of contractor designs is not available.

Enumeration of DOD integrated circuits needs is complicated by the fact that its military systems IC requirements occur in two phases.

In the first phase, the development and special systems period, DOD needs access to the most advanced technology ICs for new science and technology (S&T) and R&D programs and for some sensitive systems. Assured access to the most advanced IC technology is essential for evaluating new concepts and capabilities and for the design, development, and testing of new products. Without ongoing access to evolving microelectronics technologies,

continued advancements in warfighting will not be achievable. For example, for many DOD, service and agency S&T and early development phase projects access to the smallest-feature-size, highest-speed, and most-complex processing devices holds the promise of allowing substantially upgraded weapon system and intelligence product performance levels. Equally, DOD classified and sensitive systems often require performance that demands continuous and rapid access to the most advanced IC technology.

In the later second phase, the systems production phase, a different problem arises.[23] Based on data supplied by the ODUSD(IP),[24] it appears that by the time complex systems developed for the DOD enter production, the IC technology incorporated in those designs has already become mainstream or even obsolete. In many cases, components procurement officials for new DOD production systems find that the ICs incorporated in their designs are at or nearing the end of life and are about to be out of production. In this phase, the problem is access to old technology.

DOD ACQUISITION OF TRUSTED MICROELECTRONIC COMPONENTS

Throughout the past 10 years, DOD's need for classified devices has been satisfied primarily through the use of government-owned, government- or contractor-operated, dedicated facilities such as those operated by the National Security Agency (NSA) and Sandia. The rapid evolution of technology has made the NSA facility inadequate to perform this mission; the cost of continuously keeping it near to the state of the art is regarded as prohibitive. The Sandia facility, while its mission does not require leading-edge commercial processing capability, is now upgrading its facility to meet DOE's

23. By the time systems now in design go into production today's state of the art technology, 90 nm CMOS, will have become an "older technology." Fabrication lines to make them, however, will still need 300 mm equipment to produce wafers.
24. Based on ODUSD(IP) sponsored study by DCMA. DCMA polled 23 leading electronics suppliers for DOD to characterize the number and types of devices used in DOD products.

stockpile stewardship, engineering, and process development requirements. These facilities historically provided classified or highly sensitive products, but did not address the need for "trusted" supplies for a larger set of DOD weapon system devices; there were sufficient U.S. firms willing and able to satisfy the then–state-of-the-art needs.

There is no longer a diverse base of U.S. IC fabricators capable of meeting trusted and classified chip needs.

DOD has initiated a trusted foundry program to provide, in the interim, a source of high-performance ICs in accordance with the overall defense trusted integrated circuit supply (DTICS) mandate. DOD has contracted for these services on a "take-or-pay" basis.[25] More information on the trusted foundry program can be found in appendix F.

At this time, a single foundry contract has been let for leading-edge fabrication (tier 1)[26] services with IBM. No foundry contracts have been negotiated with tier 2 and 3 fabricators; however, the larger number of fabricators available to produce ICs with processes one or more generations behind the leading edge has resulted in supplier competition to participate in the program. Sources of the older tier 2 and tier 3 technologies are much more available; however, a longer-term concern remains when the current tier 1 technology becomes tier 2 and there are few U.S. facilities capable of practicing it. The specific qualifications required of a foundry to be designated "trusted" are the province of the trusted foundry program and DTICS.

25. Presentation to the Defense Science Board Task Force on High-performance Microelectronics by Chuck Varney, Chief, Trusted Access Program Office May 20, 2004.
26. For purposes of the Trusted Foundry Program, the term "Tier 1" refers to a foundry having the state-of-the-art (leading edge) of commercial wafer fabrication technology. At this time, the leading edge is a CMOS process with 90 nm minimum critical dimensions. "Tier 2" is taken to refer to a foundry capable of processing wafer 2 to 4 generations behind the leading edge (now CMOS with 130, 180 or 250 nm critical dimensions), "Tier 3" refers to foundries with wafer processing capabilities even further behind.

The objective of the DOD trusted foundry program is to establish trusted, leading-edge fabrication capabilities to produce microelectronics components for sensitive defense and intelligence community applications.

The trusted foundry program allows for chip fabrication of DOD components determined to require acquisition from trusted sources in United States–owned and United States–located commercial facilities, and perhaps those of selected, trusted allies, under contract to DOD. Security controls allow for clearance of personnel necessary to protect the product at a maximum of DOD Secret. Wafer processes available through the trusted foundry will follow the commercial technology roadmap stabilized through commercial production volumes. Accelerated turnaround times are available, provided they are precoordinated with the foundry. A certain number of accelerated turns have been prepaid, and additional ones can be purchased. Life cycle for the processes is based on the commercial viability of the process. Typical processes will last 10 years. In addition, the foundry will provide a two-year notification for any of the processes it plans to retire. All programs that have ordered parts with that process will be notified in order to provide them the opportunity to order an end-of-life buy.

Surveys are being planned to develop additional tier 1 sources to ameliorate the risks inherent in single-source manufacture. However, there are presently only a very few facilities that can qualify as leading-edge processing facilities.

Legacy parts have been produced effectively by the Defense Microelectronics Activity (DMEA) and under its aegis by several manufacturers who specialize in producing older technology parts. Future legacy replacement parts (both COTS and non-COTS), however, will require much more sophisticated technical skills. Any redesign of legacy parts to meet continuing replacement needs provide new opportunities for adversary mischief.

The types of devices that are most at risk of corruption are mission-critical, application specific integrated circuits (ASICs), including digital or mixed-mode digital/analog components and

fully custom integrated circuits and gate array class devices. While these devices are potentially corruptible, they provide superiority in functionality, speed, and power consumption. Ensuring that these are truly trusted devices is of the utmost importance.

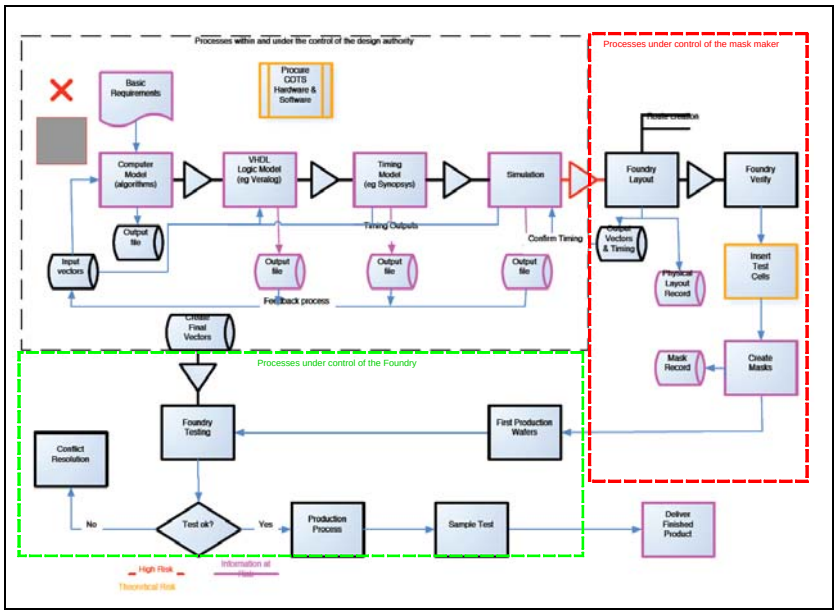


Figure 5

The design of an ASIC device is a complex process involving a team of engineers that includes specialists in software, firmware, system architecture, timing, circuit and device design, and testing. In Figure 5, the ASIC design is enclosed in the black dashed line and mask making in red. The activities in these stages are those that entail direct access to the chip design database and are thus very high risk, as is delivery of the completed chips. The green box encloses the fabrication steps under control of the foundry, where unauthorized process changes and outright substitutions are also possible. The green-enclosed area is the portion of the ASIC chip design and fabrication chain the Trusted Foundry Program is intended to protect.

STANDARD AND CUSTOM PARTS

The semiconductor world can be divided into two broad producer segments – standard (commodity) and custom products. Standard products are sold to many customers for use in many applications; custom products – ASICs – are designed, manufactured and sold to one customer for specific uses. The economic models for suppliers and customers in these two segments are very different. While a great deal of attention is paid to securing trusted ASIC supplies for the DOD community, questions must also be asked about the future sources of standard products.

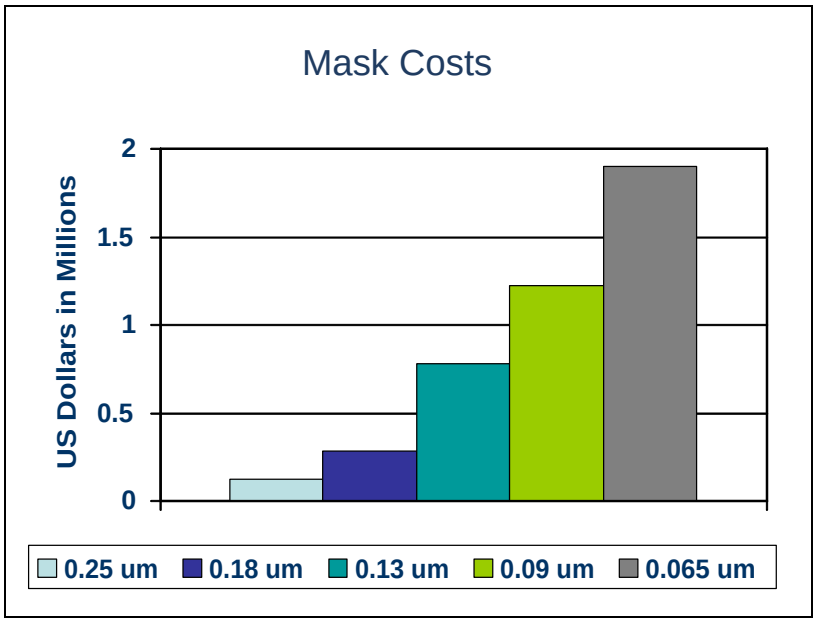


Figure 6

Custom IC Trends and the Commodity Manufacturing Model

Fixed costs are the barrier to continued use of large numbers of custom ICs in limited-volume applications such as military systems. Dealing with the complexity of state-of-the-art chip designs that may contain more than 50 million transistors is in itself costly.

Additionally, the mask costs for fabricating chips using advanced technologies can be overwhelming. The cost of a mask set for a 90 nm design now exceeds $1 million, and future process-generation mask costs will be even more expensive.

Since it is clear that the general tendency is to manufacture leading-edge semiconductor products outside the United States and the fixed costs of ASIC design and fabrication are skyrocketing, a clear trend is emerging for designers to use as few custom semiconductor products as possible; instead, they employ programmable standard products. Semiconductor standard products whose functionality can be changed by software programming, as in the case of microprocessors (MPUs) and digital signal processors (DSPs), or hardware programmability, as in the case of field programmable products such as field programmable gate arrays. While these standard products will also increasingly be manufactured offshore, their functionality is mostly controlled by the user, it may be impossible to independently secure that functionality.

Programmable parts have more intricate designs, which make them difficult to validate (especially after manufacturing) and thus more subject to undetected compromise. Thus, it is important that programmable components be "trustable," though only to a degree that is commensurate with their application. In a small subset of cases, the degree of trust required might be so high that all steps of the design, manufacturing, and supply chain must be thoroughly secured, for example, through the use of a trusted foundry. However, in many cases use of a trusted foundry will be infeasible and/or it will be sufficient for the DOD to "trust" high-volume "standard" parts that are manufactured commercially and obtained via a supply chain that limits the risk of post-manufacture tampering.

The key to success in all commodity businesses, including manufactured programmable standard products and memories, lies in producing very high volumes of the same design very efficiently. This precept has led to factories designed around very large wafers, optimized for specific product designs. Cost is reduced by eliminating any variations in process and product. This is the manufacturing model for all major IC producers today.

Such manufacturers (especially memory and standard processor producers) are not amenable to custom product production, putting them at odds with DOD's leading-edge technology, custom-design, small-volume product needs.

New Custom IC Production Equipment and Methods

While many future defense systems will be designed using commodity and programmable standard products, there are many instances where use of custom products is mandatory. Low-power, high-speed subsystems, analog front ends and power amplifiers, electronically steered antennas, and special cryptographic applications all demand unique parts. However, current semiconductor manufacturing is a very capital-intensive business, with state-of-the-art wafer fabrication factories (fabs) costing in excess of $3 billion today.[27] Furthermore, the current approach to manufacturing requires that a process be qualified and stabilized, i.e., many test wafers must be run through the system before it yields working parts. The resultant state of the art is a batch process in which expensive fabs are designed to make large quantities of standard products, which is at odds with DOD requirements for leading-edge technology products in small volumes. Although commercial foundries subsidize their customer's prototyping efforts, they do so in the hope of attracting designs that will some day enter volume production and are unlikely to extend similar terms to designers whose total lifetime production requirement may only amount to a few wafers.

The IC industry situation is analogous to the pre-1970s steel industry, where emphasis on huge, standard product mills froze out the U.S. specialty steel business. A subsequent business disaster prompted by low-cost imported steel led to a reexamination of steel production methods, which resulted new technology underlying the mini-mills that now flourish in today's U.S. steel industry.

27. While the cost of today's leading edge production fabrication plants is approaching $3B, the investment required for future facilities is expected to double every other technology generation. The conversion to 450 mm wafers forecasted to take place in five years will add still more to fixed plants costs.

A similar reexamination of integrated circuits manufacturing is needed to assure continued ability economically to design and produce custom parts at the leading technology edge. An industry need for the same service is also growing. Today, there is little commercial requirement for such capability, just as there was no requirement for the mini-mills until an economic collapse in the U.S. steel industry forced the issue. Lacking a business disaster, DOD's need for custom microelectronics trusted sources is pressing, and therefore the burden of prompting development of this capability falls to DOD. The DOD does not own the complete burden for action (for instance ASIC manufacturers and the semiconductor manufacturing equipment industry must participate), but certainly the leadership burden must be borne by DOD.

The tiered trusted foundry approach offers a relatively short-term solution to trusted leading-edge custom circuit supply. In the long run, it is not a realistic approach to satisfying DOD and the commercial industry's needs. New methods and equipment concepts must be found that make custom circuit fabrication economical.

SEMICONDUCTOR MANUFACTURING EQUIPMENT EXPORT CONTROLS

Dual-use technology exports that pose national security or foreign policy concern are regulated pursuant to the Export Administration Act of 1979. Advanced semiconductor manufacturing equipment and technology are regarded as sensitive, and export to China requires issuance of an export license by the Department of Commerce (DOC). Applications for export licenses are reviewed by the DOC as well as the Department of Defense and the State Department. Decisions to grant or not grant a license are determined on a case-by-case basis.[28] Since the end of the cold war, U.S. export

28. The Department of Commerce also has an export status called a "License Exception." A License Exception, once granted to an semiconductor manufacturing equipment (SME) supplier allows that supplier to ship a specific class or model of SME covered by the license exception to a particular end user (e.g. SMIC in China) without having to ask for an individual license for each piece of equipment. The equipment is shipped without delay.

controls have become less effective in restricting the flow of advanced Semiconductor Manufacturing Equipment (SME) and design technology and equipment to China. During the cold war, the United States and its allies collectively restricted exports of sensitive dual-use technologies to the Warsaw Pact countries and certain others, including China, through the Coordinating Committee for Multilateral Export Controls (CoCom), a treaty organization. Under the CoCom regime all participating countries agreed not to export certain prohibited dual-use items to subject countries, and to secure unanimous preapproval with respect to export of prohibited items. CoCom was replaced in 1996 by the Wassenaar Arrangement, a non-treaty, voluntary system for the coordination and sharing of information with respect to the export of sensitive technologies. The Wassenaar system differs from CoCom in fundamental ways:

- Under Wassenaar, each country commits only to ill-defined self-restraint with respect to export of sensitive technologies. (Signatories agree not to export technologies that would result in the development or enhancement of military capabilities that undermine regional and international security.)
- The Wassenaar controls are not aimed at exports to any particular country or group of countries, and a number of signatories have rejected the notion that exports to China could undermine regional and international security.
- No Wassenaar member has veto power over any other member's decision to export a particular item to a given country (i.e., each country retains its own "national discretion" concerning exports).
- Any of Wassenaar's 33 members can veto proposals for the adoption of new collective restrictions.

Advanced semiconductor manufacturing and design equipment with roughly comparable performance characteristics is produced in a number of Wassenaar signatory countries. As a result, under the Wassenaar regime a Chinese buyer who cannot obtain desired equipment items from U.S. makers because the Department of

Commerce has not granted an export license can often acquire comparable equipment from competing sellers based in Europe or Asia who are able to obtain licenses from their governments. This situation has led U.S. producers of SME and design tools to complain that U.S. export controls are undermining their international competitiveness by limiting their access to the world's fastest-growing market for their products – China – while failing in their basic purpose of limiting Chinese access to advanced semiconductor technology. On several occasions, the U.S. government has sought to persuade other Wassenaar members to restrict exports of SME to China, but has been rebuffed. The U.S. government has been further hampered by inadequate information with respect to the types of SME and design equipment and technology that are currently available to Chinese enterprises from sources outside the United States.

Taiwan, although not a Wassenaar member, maintains its own legal controls on the export of sensitive SME and design tools to China, as well as restrictions on the movement of certain personnel with semiconductor process and design skills. However, with the advent of numerous Taiwanese-owned and Taiwanese-managed foundries on the mainland, concerns have arisen about the potential flow of sensitive equipment and technology from Taiwan to the mainland.[29]

STANDARD CHIPS WITH PROGRAMMABLE HARDWARE AND/OR SOFTWARE

Defense system electronic hardware, like that used in commercial applications, has undergone a radical transformation. Whereas custom circuits, unique to specific applications, were once widely used, most information processing today is performed by

29. In March 2002 the Hsinchu District Prosecutors Office was reportedly investigating allegations that a former TSMC manager in charge of 12-inch wafer development had sold trade secrets via e-mail relating to 12-inch wafer process technology to an unidentified Chinese firm. The same month Taiwanese legislators charged the UMC had illegally sold SME to Chinese companies based in Shanghai via an intermediary firm incorporated in the Cayman Island, *Taipei Times* (March 16, 2002).

combinations of memory chips (DRAMs, SRAMs, ROMs, etc.), which store data (including programs), and programmable microchips, such as Programmable Logic Arrays (PLAs), central processors (CPUs), and digital signal processors (DSPs), which operate on the data. Of the two classes of parts, the latter have more intricate designs, which make them difficult to validate (especially after manufacturing) and thus more subject to undetected compromise.

Structured ASICs are mask-programmable alternatives to pure ASIC parts. They consist of regular logic arrays with support interconnection (clock, power, and ground) fabricated as standard products. Multilayer interconnections are added later, possibly under trusted conditions, to "personalize" the array for their application-specific functions. The structured ASIC offers a relatively quick turnaround option for moderate-volume IC needs at some cost in density, speed, and power.[30]

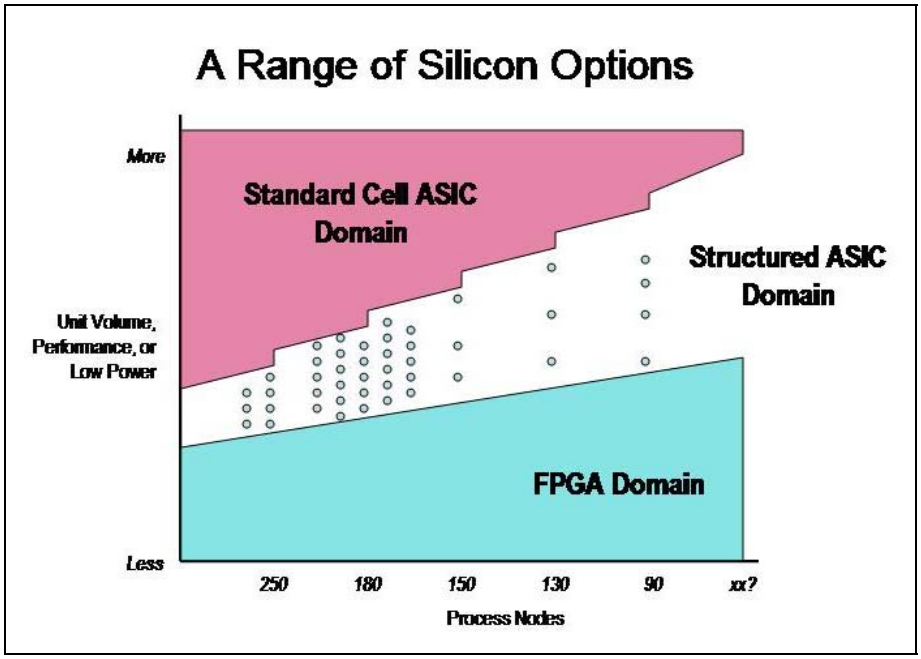


Figure 7

30. Information provided by Lightspeed Semiconductor.

Field programmable gate arrays are complex standard products whose function is determined at the point of use by patterns stored in a read-only memory (ROM). As with structured ASICs, logic units are built into the chip along with programming circuits, so that FPGA function is under the control of the user, and can be changed in the field, if desired. FPGAs offer the ultimate in fast turnaround time, since they are configured in the application itself. Although very complex, FPGAs are now available with embedded memories, digital signal processors (DSPs), and microprocessors (MPUs). FPGAs are slower and dissipate more power than ASICs.

The relative ranges of application of ASICs, structured arrays, and FPGAs are shown in figure 7.[31] Appendix G gives a comparison of system cost and performance with ASICs and with FPGAs. ASIC variable cost per unit is generally less than that of FPGAs; however, the high nonrecurring costs of ASICs (layout, mask, and test costs) make FPGAs more cost effective in low-volume production applications.

In many cases, use of a trusted foundry (particularly for commodity ICs) will be unfeasible. It will have to be sufficient for DOD to "trust" high-volume "standard" parts that are manufactured commercially and obtained via a supply chain that limits the risk of postmanufacture tampering.

Defense systems will always rely on a few custom parts, especially where speed, analog, or power considerations compel their use; however, economy and flexibility dictate use of standard programmable ICs wherever possible.

Placing emphasis on the use of "standard" programmable parts is attractive for four reasons:

- These parts are manufactured in high volume. Thus when DOD and its contractors use them, they benefit from the economies of manufacturing scale characteristic of commodity parts.

31. Provided by Xilinx, Inc.

- Software to program these devices are much, much easier to develop than the equivalent custom IC designs.
- U.S.-based companies lead in the design and manufacturing of programmable standard parts: Texas Instruments (TI) is a leader in DSPs; IBM and Freescale (formerly Motorola) lead in CPUs and systems on a chip (SOC) with embedded processors; Xilinx and Altera are leaders in FPGAs; and Intel is a leader in CPUs and MPUs.
- Hardware programmable standard products such as PLAs and FPGAs are particularly important in meeting the custom function needs of military systems. The performance gap (in speed and power dissipation) between PLAs and FPGAs and ASICs, once a significant barrier to use of programmable logic arrays, continues to narrow, making hardware programmable devices an attractive choice for many custom applications. Simultaneously investing in further closing this gap and in new, efficient programming algorithms for these devices may allow the DOD to retain information superiority without requiring as wide an assortment of ASICs as in the past.

Although U.S.-based leadership does not in and of itself assure the trustworthiness of these parts, it does put the DOD in a position superior to that of potential adversaries, whose systems rely on U.S.-based suppliers and/or inferior parts procured abroad. This advantage accrues not only to fielded weapon systems, but to all aspects of the defense community and of U.S. national infrastructures.

U.S. leadership cannot be taken for granted, especially given the global consolidation underway in the semiconductor industry. Thus, it is especially disconcerting that U.S. government research funding in this area has continued its decline as a percentage of the GDP as shown in the figure below.

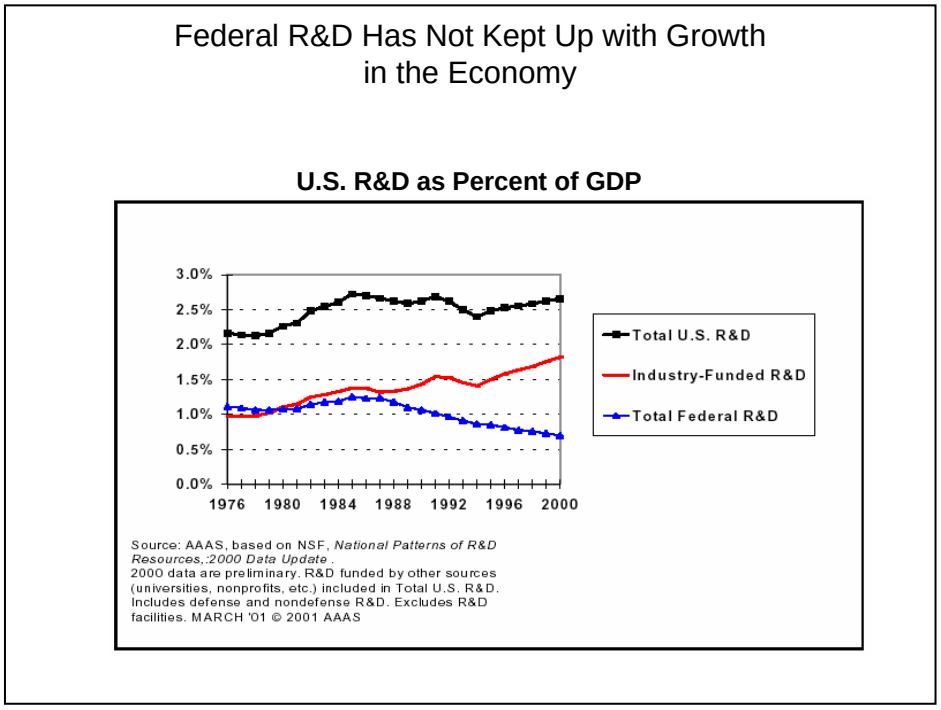


Figure 8

DOD-UNIQUE TECHNOLOGIES

Defense systems, by the nature of their functions and use environment, require technologies for which there is no wide commercial demand. The most widely known of these "special" technologies is that of radiation-hardening of circuits to allow their operation and survival through a nuclear event. Similar unique technologies include low-power and countertamper techniques. Research and development for these special technologies is supported almost entirely by DOD through Defense Threat Reduction Agency (DTRA), NSA, and similar mission agencies.

Although commercial processes are evolving coincidentally toward satisfying some DOD special needs, such as radiation tolerance, there remains an irreducible need for special fabrication. Maintaining viable supply sources for microelectronics parts incorporating DOD-unique technologies is part of the trusted supply

problem. Commercial facilities lack the unique processes required to meet DOD-unique needs.

The DOD Radiation-Hardened IC Production Program is a useful first step in meeting DOD special needs; however, challenges remain in keeping the dedicated fabrication facilities supported under this program up-to-date as commercial processes advance.

ADVERSARIAL CLANDESTINE OPERATIONAL OPPORTUNITIES

Because of the U.S. military dependence on advanced technologies whose provenance is progressively more offshore, opportunities for an adversary to clandestinely manipulate technology used in U.S. critical microelectronics applications are enormous and increasing. In general, a sophisticated clandestine service will develop opportunities to gain close access to a target technology throughout its lifetime. If access is early in a product's life cycle, such as in the design phase, the adversary has the option of affecting every unit produced. More narrowly focused targeting can be accomplished later in the life-cycle. An example of a surgical operational approach was effectively used by the Soviets in the early 1980s by intercepting typewriters destined for the U.S. embassy in Moscow and making a clandestine modification. This modification allowed the Soviets to secretly obtain copies of every document typed on the altered typewriters. [32]

Increasingly, as microelectronic component product design and production move out of direct United States control, adversaries are able to acquire life-cycle operational access to U.S. key hardware technologies. In many cases, DOD program managers and U.S. industry inadvertently provide access to potential enemies as a result of their attempts to cut costs, manage schedules, and provide state-of-the-art technology by moving critical design and production steps offshore. Unfortunately, this strategy provides opportunities to deeply embed subversive constructs into these components and systems that could compromise the security requirements of critical

32. Presentation to the Defense Science Board Task Force on High-performance Microelectronics by a DOD representative, May 20, 2004.

applications (confidentiality, integrity, or availability). Today, offshore engineers design, develop, test, fabricate, remotely maintain, integrate, and upgrade some U.S. defense hardware and software. Regrettably, the United States currently has no effective strategy to weigh the obvious cost and time advantages of outsourcing offshore against the potential of component subversion.[33]

If real and potential adversaries' ability to subvert U.S. microelectronics components is not reversed or technically mitigated, our adversaries will gain enormous asymmetric advantages that could possibly put U.S. force projection at risk. In the end, the U.S. strategy must be one of risk management, not risk avoidance. Even if risk avoidance were possible, it would be prohibited by cost. Factors affecting the risk management calculation are numerous, complicated, and interdependent. They include

- Ability of an adversary to gain life-cycle access and keep such access secret
- Given access, an adversary's capability to alter a component such that the alteration is difficult to detect and to attribute
- The adversary's willingness to exploit such an opportunity
- The benefit to the adversary
- The impact of a compromise on the United States
- Capability of the United States to detect a modification
- Capability of the United States to attribute the modification
- Consequence to the adversary if the modification is detected and attributed to them

33. Some of these activities may be contrary to long-standing International Traffic in Arms Regulations (ITAR) export controls. While the U.S. has an extensive set of laws and regulations governing export of critical technologies, comprehension of their importance and application is not widespread.

- Ability of the United States to limit the life-cycle access opportunities, for instance, to a trusted foundry
- Alternate approaches available to the adversary in achieving equivalent impact (i.e., software modification)
- Cost

CONCLUSION

The Department of Defense and its suppliers face a major integrated circuit supply dilemma that threatens the security and integrity of classified and sensitive circuit design information, the superiority and correct functioning of electronic systems, system reliability, continued supply of long-system-life components, and special-technology components.

- The department must solve this problem together with the rest of the defense community (i.e., defense suppliers). With few exceptions, today's commercial industry will not perceive the same threats as DOD and will not adjust its operations to meet small-manufacturing-volume military needs.
- DOD should also play an advocate role in U.S. attempts (through the U.S. Trade Representative (USTR), the Committee for Foreign Investments in the United States (CFIUS) process, Department of State (DoS), National Security Council (NSC), Department of Transportation (DoT)) to achieve trade and economic equity in the global semiconductor industry in order to discourage the industry's migration abroad and incentivize the installation of future advanced technology integrated circuit manufacturing and design in the United States.
- DOD's microelectronic problem is most severe at the leading technology edge and in special technologies,

although some risk is inherent in legacy part redesigns.

- Additional study by both the DOD and its suppliers is needed to determine how best to assure supplies of obsolete parts needed for system repair and replacement.
- Although there have been concerns about isolated supply problems (e.g., radiation-hardened and obsolete parts supplies), the full integrated supply problem has emerged onto the acquisition agenda and is only now being fully identified. DOD lacks a stable long-term investment, technology, and acquisition strategy capable of meeting its and its suppliers microelectronic component supply needs. Attempts to deal with microelectronics supply issues have been limited to isolated efforts to date.
- DOD lacks a long-term plan for the preservation of U.S. information superiority, which is a cornerstone of U.S. national security. The department must either develop such a plan or be prepared to surrender this advantage, i.e., identify the alternative means by which national security will be assured in a regime of information inferiority.

This conclusion is a call for the U.S. government in general, and the DOD and its suppliers specifically, to establish a series of activities to ensure that the United States maintains reliable access to the full spectrum of microelectronics components, from commodity and legacy, to state-of-the-art parts, and application-specific ICs special technologies. These activities must provide assurance that each component's trustworthiness (confidentiality, integrity, and availability) is consistent with that component's military application.

Over time, semiconductor design and production will almost certainly become more, not less, globalized, making risk mitigation strategies that rely strictly on domestic design and production increasingly difficult, if not impossible, to implement. Commercial firms may be eager to contract design and production services, but

they may be subject to overriding national control in times of stress. While a trusted leading-edge supplier concept may provide near-term risk reduction, over the long term, additional risk mitigation and risk management strategies must be developed.

Acquisition efforts must be buttressed by both legal and technical efforts to protect U.S. technical leadership and intellectual property in the microelectronics domain. This includes maintaining and nurturing the U.S. electronics skill base through continuing, stable research funding (see appendix D). Research is particularly important at this time, as the traditional growth of IC capability shows signs of slowing; new device concepts and structures will be needed to continue device advances on which future defense systems concepts are predicated. The alternative is a future in which the same hardware technology is universally available, to friend and foe alike.

In the long term, if potential adversaries become leaders in microelectronics technologies, the United States may find itself the target of "reverse-ITAR" restrictions on critical electronics capabilities. The United States must maintain sufficient control and influence over microelectronics research, design, fabrication, and testing to satisfy U.S. microelectronics requirements for the indefinite future.

Developments in the semiconductor industry parallel similar trends in the software field. This similarity should be no surprise, since both fields deal with inherently complex designs; they require technically similar design techniques and tools. Additionally, software is the key to how hardware behaves; a matching subversion of a combination of hardware and software (especially in the case of programmable logic devices [PLDs] and field programmable logic [CPLDs[34] and FPGAs]) could be impossible to detect. Other technologies, such as printed circuit boards, may be affected, but to a much lesser extent.

34. Complex Programmable Logic Devices, or CPLDs, are predecessors of FPGAs which are suitable for simple logic applications.

This page intentionally left blank.

RECOMMENDATIONS

Ameliorating the threats to trusted and assured DOD supplies of microelectronics components will require a multipronged approach. Pursuing only one or two initiatives will not suffice. Acquisition, technical, and trade actions are all needed.

Supplies of trusted microelectronics components are important to the broad spectrum of the U.S. electronics industry, both military and civilian. From a national security standpoint, however, greatest concern lies in microelectronics supplies for defense, national infrastructure, and intelligence applications. Assuring supplies of trusted microelectronics components for defense systems use requires actions well beyond the scope and magnitude of those that can be mounted by a single defense supplier, or by the entire defense contractor industry. Addressing this problem is a uniquely governmental function. DOD is charged with the defense of the United States, a mission that depends heavily on microelectronics. While actions to mitigate threats to U.S. microelectronics trusted and assured supply require concerted action by many government agencies and departments, DOD has a major stake in reaching solutions to these problems. The task force considers DOD the logical steward to lead, cajole, and encourage a national solution to this critical problem, regardless of which arm of government must act. The task force also sees DOD as the logical U.S. government point to convene supplier, subsystem, prime and government users, and commercial interests, to address the recommendations in this report.

This task force's recommendations are ordered from general to specific. The overriding logic of these actions begins with the realization that maintaining trusted and assured supplies of microelectronic components based on a healthy, multisource U.S.-resident (or trusted ally) commercial design and manufacturing capability at the leading edge of technology requires DOD leadership (recommendation 1). On a broad scale, economic and trade conditions for semiconductor manufacturers operating in the United States must be as attractive as those for manufacturers operating

elsewhere (recommendation 2). The department should estimate the number and varieties of microelectronic components that require trustworthiness as an aid to planning the size and scope of the Defense Trusted Integrated Circuits Strategy[35] (recommendation 3). Access to the necessary design and manufacturing capability requires that DOD purchase products and services from leading-edge semiconductor firms in a way acceptable to the government, its systems contractors, and to the component suppliers. DOD needs a focused, tailored acquisition plan, driven by a long-term vision of its semiconductor needs, to establish the basis, policy, and operating guidelines for DOD-enabled access to trusted foundry services by the department, its contractors, and others. (For instance, the status of foundry-supplied components as government-furnished equipment must be clarified as well as payment policies. [recommendation 4]). Cost and manufacturing technology trends are making design and fabrication of limited-volume ASICs prohibitively expensive. New low-volume chip manufacturing models and fabrication equipment are required if future defense systems are to have unique microelectronics hardware capabilities at a reasonable cost. The same requirement for economical, modest-volume ICs is developing for future commercial products. A reexamination of economic models for producing low-volume products will require a joint government - industry program to develop new, more flexible factory technology capable of meeting both defense and commercial needs (recommendation 5). The United States and its allies still maintain regimes of export controls for defense-critical and dual-use technology and equipment as one approach for limiting some technology transfers to potential adversaries (recommendation 6). Recommendations follow addressing specific technologies unique to use of programmable "standard" components (such as PLAs, MPUs and DSPs), defense applications and assurance of component trustworthiness (including design techniques), DOD-unique technologies, and countertamper proficiency (recommendations 7, 8, and 9).

35. Memo from the Deputy Secretary of Defense, "Defense Trusted Integrated Circuits Strategy", dated October 10, 2003, Ref. U16619/03 - see Appendix C.

RECOMMENDATION 1 – COMMIT TO DOD LEADERSHIP

DOD, prompted by the secretary and the undersecretary for acquisition, technology and logistics, must lead in guaranteeing its needs are supported by ensuring that the United States industry transforms and enhances its present position in onshore microelectronics. Providing for assured supplies by DOD's contracts with today's trusted foundries will help solve the immediate problem, but this measure is only temporary; it will not address the structural issue of funding the research that will sustain our information superiority. Long-term national security depends upon U.S.-based competitiveness in research, development, design, and manufacturing. Many actions required for this guarantee, however, are beyond the scope and function of the department.

DOD should advocate that a strongly competitive U.S. semiconductor industry is not only a DOD objective but also a national priority. Because the U.S. share of the world's leading-edge semiconductor manufacturing has declined, and because research and development is closely coupled to manufacturing leadership, the United States will soon start to lose its R&D skill base if its onshore manufacturing does not remain vital. Sustaining microelectronics leadership is essential to U.S. defense systems' world dominance; sustaining microelectronics must therefore be a national security objective, understood by both the administration and Congress.

The task force recommends that DOD senior officials

- Take a leadership role in establishing trusted foundries in the United States for general use by military and critical infrastructure component manufacturers.
- Recognize that the long-term solution to the problem of meeting leading-edge defense microelectronics needs depends on countering today's economic reality of migration of integrated circuits manufacturing from the United States.

- Understand and vigorously communicate the consequences of failure to act to retain U.S. trusted and assured microelectronics supply and design.
- Advocate that Congress and the administration embrace economic incentives and steps to attract those with the best technical skills to the field and the United States. These measures are required to make the United States an attractive place to manufacture semiconductors, related manufacturing equipment and materials.
- Involve:
  - The White House, including appropriate councils and offices
  - Commerce and Labor Departments, also the USTR
  - Key congressional committees (both chair and minority leader)
  - Industry

RECOMMENDATION 2 – LEVEL THE PLAYING FIELD

As a first step the task force recommends that the secretary of defense, the USD(ATL) and the secretary of homeland security prepare a special briefing for the national security advisor and encourage him or her to take a key role in implementing the measures detailed in this recommendation to slow the migration of the microelectronics industry and enable it to strengthen its future in the United States.

To assure the ability of the DOD to access leading-edge trusted manufacturing facilities, the United States needs a broad national effort to offset foreign polices designed to encourage movement of leading edge semiconductor manufacturing facilities to offshore locations. In an ideal world, locational investment decisions would be based on commercial and economic factors, not government incentives, but we do not operate in an ideal world. A coherent U.S.

policy response is necessary to counter the extensive intervention by foreign governments to encourage local investment in the semiconductor industry. Such a response will require government policies that offset foreign incentives for manufacturing investment. The federal government needs to determine its role, if any, in assisting various states in developing their incentive packages. States should also strive to ensure that their permitting processes are responsive to business timelines.

The U.S. government must vigorously support compliance with World Trade Organization (WTO) rules. The recent, apparently successful, resolution of the U.S. complaint with regard to China's discriminatory VAT is a model for U.S. responses to other foreign practices that are inconsistent with WTO rules. The U.S. government should monitor China's compliance with Part 1.7.3 of its protocol of accession to the WTO, which provides, among other things, that China will not enforce local content requirements, foreign exchange balancing, or performance requirements of any kind, including technology transfer. The U.S. antidumping and countervailing duties laws should be enforced where appropriate.

Intellectual property (IP) rights are fundamental to innovation, and while China has passed laws to protect IP, the Chinese government must take steps to guarantee that these laws are fully enforced to ensure that Chinese foundries are not producing chips and using processes that violate others' IP rights.

The Department of Defense and the U.S. intelligence agencies should become more actively involved in decision making by other agencies of the U.S. government that have the potential to significantly affect the U.S. defense microelectronics industrial base. In particular, the defense community should make its concerns known with respect to trade issues affecting microelectronics when the Office of the U.S. Trade Representative conducts interagency reviews of those issues and with respect to inward foreign investment decisions under consideration by the Committee on Foreign Investment in the United States (CFIUS). When the resolution of such issues in microelectronics have the potential to directly affect U.S. defense capabilities in microelectronics, informed

high-level participation by DOD and the intelligence agencies is essential.

University and independent laboratory work has played an important role in microelectronic history in that it has sown the seeds for major technological shifts. Much of the basic work in advanced lithography, novel computer architectures (such as the Reduced Instruction Set Computer [RISC]) and in development of computer design aids, without which complex IC circuit and process design would not be possible, arose from such research efforts. Industry research, while healthy and well-funded, excels at extension of existing technological trends (e.g., efforts promoted by the International Technology Roadmap for Semiconductors[36]). At a time when the effectiveness of conventional approaches to the extension of Moore's Law are nearing their end, new ideas are essential to continue the progress on which the industry and future military systems depend.

The United States must increase its university research funding to ensure that it remains an attractive and competitive location for the most talented students and faculty from around the world in this field. The National Science Foundation (NSF) has been a major supporter of university research in the physical sciences. The NSF Authorization Act of 2000 authorized a doubling of NSF budgets over a six-year period. The act includes specific increases in nanotechnology and networking and information technology. Congress should appropriate the funds necessary to achieve the NSF Authorization Act's goals.

The intelligence agencies should continue to monitor the global state of the microelectronics technology to determine where additional effort is required to keep the United States ahead of, or at least equal to, the world state of the art in critical fields.

36. *International Technology Roadmap for Semiconductors*, jointly sponsored by the European Semiconductor Association, the Japan Electronics and Information Technology Association, the Korean Semiconductor Industry Association, the Taiwan Semiconductor Industry Association and the Semiconductor Industry Association.

The military service research arms have also contributed major research support to U.S. universities and research laboratories. Their support has been for projects more aligned with DOD needs. Support for microelectronics at Air Force Office of Scientific Research (AFOSR), Office of Naval Research (ONR), and Army Research Office (ARO), however has dwindled over the past decade. These levels of funding should be increased commensurate with the increases planned for NSF.

As a result of recommendations by the Semiconductor Technology Council chaired by Dr. Craig Barrett, President and CEO of Intel, the Focus Center Research Program was instituted in 1999. This effort is focused on long-range research with emphasis on discovery in areas where evolutionary R&D may not find solutions. Five focus centers have been established with 30 universities participating.[37] To date, industry has provided the majority of the support of the program, with the DOD contributing additional funding and providing program management expertise through DARPA. DOD funding needs to keep pace with industry contributions. NIST is best positioned to focus research on many of the metrology challenges identified in the International Technology Roadmap for Semiconductors. When it was established in 1994, the NIST Office of Microelectronics Programs was to start at $12 million in annual funding and grow to $25 million. This level was not achieved, but this task force considers this activity an important contribution to the national microelectronics supply issue.

The United States must ensure that the American workforce is the most competitive in the world. Recent initiatives begun in math, science, and engineering education at both the K-12 and university levels included in the NSF Authorization Act must be adequately funded if the United States is to increase the number of citizens pursuing math, science, and engineering degrees. The "No Child Left Behind" Act must be adequately funded if the accountability and standards goals are to be achieved. Foreign-born students who attain

37. The Center for Design and Test is located at the University of California Berkeley; The Interconnection Center at Georgia Tech; Nanoscale materials at MIT; Circuits, Systems, and Software at Carnegie Mellon; and Nanoelectronic Devices at UCLA.

advanced technology degrees in U.S. universities must be encouraged to remain in this country to help move the technology base forward. Technology is portable in the minds of these students, and their departure is our loss and others' gain.

The Department of Defense needs to solicit the support and cooperation of other government organizations to maintain the supply of U.S.-built trusted semiconductors. The USTR must monitor foreign countries with regard to practices that distort trade and investment patterns and jeopardize U.S. intellectual property issues. The NSF must be funded to boost university research in nanoelectronics and beyond.

The United States is still the leader in technology, and a sufficient supply of many trusted microelectronic components is available. The trends of the last few years, however, indicate that this will not continue in the near term unless direct action is taken in the immediate future.

RECOMMENDATION 3 – UNDERSTAND THE TRUSTED MICROELECTRONICS NEED – ENUMERATION

The DUSD(IP) is leading a DOD effort to collect component acquisition data from 23 DOD prime end item contractors.[38] In this effort, the under secretary has asked the firms to identify all ASICs included in their prime end items. Based upon preliminary and as yet incomplete feedback from this survey, DOD products entering or in production are not generally using the most advanced IC technology. Feature sizes (an indicator of process maturity) for custom ASICs in systems such as the F-22, V-22, C-17, C-130J, B-1, Apache, SH-60 and M-1 tank are generally no smaller than 0.9 microns – a 1980s-era technology. While the incompleteness of those data must be underscored, the smallest feature size found in this survey to date was 0.2 microns (early 1990s). This finding is not unexpected; disparity in product development cycle-times means that, to assure trusted sources for its in-production and in-fleet

38. Institute for Defense Analyses study of DOD Integrated Circuit Demand (in progress).

systems support, DOD will have to implement an approach that continues to provide trusted production after support IC technology generations have left production. Newer programs, such as Joint Strike Fighter (JSF), already have preplanned electronics updates, even before the system becomes operational.

DOD must also determine if other classes of ICs incorporated in its weapon systems and other key mission products require trusted sources and how many such circuits are needed. This requires that DOD identify device and technology types of microelectronics devices that require trusted sources as well as the length of time it will need such special supply arrangements. This identification must include the full range of technologies needed for DOD as well as its suppliers.

DOD must also continue its efforts to inventory current and future trusted component needs as a basis for its long-term microelectronics acquisition plans.

RECOMMENDATION 4 – DEVELOP A DOD MICROELECTRONICS ACTION PLAN

Led by the USD(AT&L), DOD and its military departments and agencies, working with their system suppliers, must develop a plan of action that encompasses both short- and long-term technology, acquisition, and manufacturing capabilities needed to assure ongoing availability of supplies of trusted microelectronic components. This plan of action requires both a vision for the long-term steady-state and an implementation plan.

Determine long-term DOD microelectronics objectives - a Vision

- During the past decade, DOD eliminated many military specifications and opted to rely, so far as possible, on commercial products and processes.

Having experienced acquisition policies based both on special and commercial standards and processes, the DOD now needs to understand, reassess, refine, and make clear its steady-state vision for assuring its microelectronics components supplies. The generation and maintenance of this vision should be assigned to the DDR&E. The task force suggests the following elements for the vision:

- Establish and publish DOD's policy reaffirming the criticality of access to advanced IC technologies and the need for microelectronics S&T and R&D funding; and define and provide guidance on a subset of microelectronics components that require special considerations for "trustworthiness." This policy should include direction as to when the department must assure COTS component trustworthiness.
- Review and determine if microelectronics S&T and R&D funding levels are consistent with new priorities.
- Institutionalize a formal approach to interagency and interdepartmental working groups, including DOD, DoE, and the intelligence community, in order to examine threats to and means of verifying trustworthiness of microelectronic components. These groups should continually evaluate the state of the art of techniques such as tamper-proof design, life testing, reverse engineering and chip and package testing for their practicality for DOD use. The working groups should pay particular attention to techniques for assuring trustworthiness of embedded processors and memories in array and "system on a chip" components.

Assign internal responsibilities and actions in three major areas in accordance with DOD's goals

1. Ensure continuous availability of microelectronic components to meet DOD needs:
   - Designate a single DOD organization (e.g., DDR&E) with responsibility to maintain the focus on microelectronic capabilities available to the DOD. This lead organization will provide executive leadership, formally tasking other DOD/OSD elements to carry out specific activities. It will have several permanent, ongoing responsibilities:
     - Create an annual, moving estimate of DOD 5- and 10-year future microelectronics needs (including processes and design methods). Collect and organize known and projected technology requirements.
     - Enhance, shape, and direct DOD microelectronics S&T budgets and RDT&E programs to assure projected requirements will be met.
     - Track and analyze microelectronics industry capabilities, including trusted technology and production capabilities (DUSD(IP)).
     - Perform outreach and industry coordination on all these tasks via external advisory groups and industry associations.
     - Arrange trusted foundry capacity as needed at all tier levels and define their funding model. Also, issue directions and policies for their use.
2. Ensure availability of trusted hardware as needed:
   - USD(ATL) must issue acquisition policy[39] requiring hardware "trustworthiness" evaluations and solutions as key, contracted performance criteria for

39. DOD 5000.2 and its Guidebook.

prime contractors. DDR&E should lead in overseeing the development and implementation of major acquisition policy elements that include

- Requiring that all programs not yet in production identify system or product areas requiring hardware trustworthiness and address these needs in program plans and system design reviews.
- Requiring that DOD PMs make trustworthiness assessments and design solutions a prime contract responsibility and that contractors utilize DOD certified trusted foundries for all microelectronics determined to require category 1 (mission critical [40]) subsystems, both classified and unclassified. The task force recommends that, as a minimum, this includes all ASICs in category 1 subsystems.
- Adding trustworthiness as a performance element in major program milestone reviews held by senior DOD acquisition leaders.

- DDR&E should also lead other DOD activities, the intelligence community, and industry participants in developing guidance and techniques for implementing this policy, including the following:
  - Informing acquisition and supplier personnel of hardware assurance "threats and vulnerabilities."
  - Establishing criteria and process guidelines for DOD programs and DOD prime contractors on how to identify or classify components requiring the highest degree of trustworthiness.
  - Developing procedures and techniques to evaluate the need for trustworthiness of each microelectronic component in defense systems.

40. DOD 8500 defines categories for mission criticality.

Include an investigation of whether field programmable gate arrays (FPGAs) and selected COTS components need trusted design or foundry process controls.

- Developing microelectronics designs that can be easily tested and evaluated.

3. Implement Acquisition Policy

- The task force recommends that DOD pursue and enlarge the trusted foundry program already underway within the department. The use of trusted foundries to manufacture components for Department of Defense systems will require changes in procedures at several levels in the acquisition process. Specific recommendations are as follows:
  - The Systems Program Office (SPO), in consultation with the prime contractor, should formally assess the level of trust required in a specific system (and its component subsystems) and document it during the system design and development (SDD) phase, with special consideration given to the application of the system and the potential damage to system utility that could be imposed by a determined adversary. Based on this high-level evaluation, the prime contractor program manager for each system should be responsible for developing and implementing procedures to meet the desired level of system trust. These procedures should include a comprehensive threat assessment and implementation of effective countermeasures at each level of system hierarchy at the time of development as well as manufacturing, fielding and life-cycle support. Regarding the flowdown of this requirement to subcontractors, the DSB recognizes that many electronic subsystem contracts are small (i.e., less than $5 million) and that the resources and knowledge base of

subcontractors may be insufficient to perform a credible threat assessment and mitigation plan. Therefore, SPO and prime contractor responsibility and leadership is essential.

- To ensure the success of (1) above, an education program must be undertaken to assure that those who are managing and developing the designs at the SPO, prime contractor, and subcontractor levels are well versed in potential threats. For example, design data and the data used in the mask-making function represent the best opportunities for the inclusion of subversive elements that can modify circuit function. Frequent peer reviews of the design are suggested as a way to detect unwanted inclusions. Design and mask data integrity is vital. Their transmission over secure lines is an integral part of the trusted foundry program.
- Integrated circuit fabrication beyond the design and mask phases offers less attractive opportunities for covert circuit inclusions; however, subtle process parameter changes can still compromise lifetime and performance in stressful environments. Consequently, it is the unanimous opinion of this DSB task force that the manufacture of mission-critical ASICs in foundries that have not been certified as "trusted" will (1) expose vital system intellectual property to potential theft; (2) increase the risk of unwanted design inclusions; and (3) possibly violate existing International Traffic in Arms (ITAR) export regulations. To mitigate these risks, the acquisition system must require all DOD laboratories and contractors to utilize the trusted foundry program for all ASICs in category 1 (mission-critical) subsystems, both classified and unclassified. Waiver requests must

have compelling justification and must be obtained through the DDR&E, and aggressive steps must be taken to increase the number of trusted foundries available for DOD and contractor use. Exceptions must also be for accommodated for the myriad of non–mission-critical prototypes developed by DOD laboratories and contractors. A draft Defense Federal Acquisition Regulation Supplement (DFARS) is included as appendix H of this report.

- As the trusted foundry program is deployed, the DOD Trusted Foundry Program Office must develop a flexible business model for contractors that evolves from government furnished equipment (GFE) and accommodates existing agreements between contractors and trusted foundry suppliers. An integrated product team (IPT) chaired by the DDR&E that includes both government and industry representatives is strongly encouraged to address these issues. The DOD Trusted Foundry Program Office must also take a leadership position in widely publicizing the trusted foundry program to SPOs, prime contractors, and major electronics subcontractors within the U.S. defense industry and intelligence community.

Radiation-Hardened Components

Special care must be taken to support military-specific microelectronic requirements such as radiation-hardened microelectronics and photonics components. DOD space and strategic missile systems, such as the transformational communications satellite, space tracking and surveillance system, and space-based radar for the Missile Defense Agency's ground-based interceptor (GBI) require radiation-hardened microelectronics and photonics components to ensure uninterrupted and long-lived

operation in either the natural space radiation environment or one enhanced by an exo-atmospheric nuclear weapon detonation.[41]

Recommendations

- Director Defense Research & Engineering (DDR&E) should continue the oversight and coordination of DOD radiation-hardened microelectronics efforts through the Radiation Hardened Oversight Council (RHOC). The RHOC should coordinate with the Defense Trusted Integrated Circuit Strategy (DTICS) Office to ensure that radiation-hardened production capabilities are qualified as trusted sources of trusted microelectronics.
- DOD should continue to sponsor radiation-hardened technology development programs covering the full spectrum of research from basic mechanisms research into new materials and design mitigation techniques to development of radiation-

41. In June 1999, the Director Defense Research & Engineering (DDR&E) formally established and chaired the Radiation Hardened Oversight Council (RHOC) to provide oversight to DOD management of radiation hardened microelectronic efforts and coordinate a corporate approach to meet the needs of planned military systems. The RHOC developed a multi-faceted strategy to ensure the long-term availability of radiation hardened microelectronics. This strategy includes: (1) the development of the Radiation Hardened Microelectronics Accelerated Technology Development (RHM ATD) program, which will satisfy DOD's need for radiation hardened microelectronics through 2015 ; (2) resources to investigate and develop alternative technologies and processes to establish a base to support the radiation hardening of microelectronics and photonics beyond the 2012 - 2015 era and (3) the development of an overarching long-term strategy to ensure the availability of hardened microelectronics post 2020 to meet DOD requirements. A key element of this strategy is to make maximum use of commercial microelectronics and photonics technologies and trusted fabrication facilities while ensuring that a viable domestic source of strategically hardened components. The basic technical approach concerning the implementation of this strategy includes the development and evaluation of material technologies with the potential to provide radiation hardening though properties inherent in the new materials; continued investigation of circuit design techniques that mitigate the damage, functional upsets, and data loss caused by the radiation environment; and long-term support of programs to maintain radiation effects core competencies.

hardened components such as nonvolatile memories to support DOD system requirements and ensure the maintenance of the RHOC roadmap.

RECOMMENDATION 5 – DEVELOP BUSINESS MODELS, TECHNOLOGY, AND EQUIPMENT FOR ECONOMIC DEVELOPMENT AND PRODUCTION OF LOW-VOLUME ASICS

Developing cost-effective technology for the design and fabrication of low-production-volume, leading-edge technology ASICs will require the combined efforts of DOD, the semiconductor industry, and semiconductor fabrication equipment suppliers. The industry's emphasis on manufacturing economies of scale has led to a manufacturing approach that is not sufficiently flexible for DOD's special circuit needs. Commercial industry is now beginning to realize a need for economical, limited IC production as well.

Developing an alternative, more flexible approach to integrated circuit manufacturing demands a thorough reexamination of business models, technology, and manufacturing equipment design. The Defense Advanced Research Projects Agency (DARPA) attempted such a reexamination in the mid-1990s through its Microelectronics Manufacturing Science and Technology (MMST) program. That program had different goals than are required today. DDR&E should now take another look at ASIC production and formulate a program to address barriers to low- to medium-volume custom IC production.

This program will require the dedicated, joint effort of all participants in ASIC production - designers, fabricators, and equipment makers. Such an effort would be similar to SEMATECH, the industry-initiated, DARPA-supported consortium. DDR&E should consider working with the existing SEMATECH or establishing a joint-effort equivalent, to seek solutions for cost-effective manufacturing of advanced-technology, custom semiconductor products in relatively low volumes. We believe this challenge can be undertaken jointly with university, industry, and government support. The leadership, however, must come from DOD. The goal should be to establish a self-sustaining business

sector that will support and sustain DOD access to low-volume, high-performance ICs.

RECOMMENDATION 6 – STRENGTHEN BILATERAL AND MULTILATERAL CONTROLS ON CRITICAL SEMICONDUCTOR MANUFACTURING AND DESIGN EQUIPMENT

The Wassenaar Arrangement covering exports of sensitive, leading-edge semiconductor manufacturing equipment (SME) is not an effective tool for assuring that potential adversaries do not have access to leading-edge IC design and wafer fabrication equipment, technology, and cell libraries. Steps to strengthen export controls include the following:

- The U.S. government should negotiate bilateral agreements or understandings with Wassenaar members in which advanced SME and design tools are made with the objective of harmonizing export licensing practices and standards with respect to China. In most cases such bilateral arrangements will involve only a handful of Wassenaar's 33 member countries. For example, only Japan and the Netherlands are significant suppliers of state-the-art lithography systems. Bilateral or multilateral agreements between the United States, Japan, United Kingdom, the Netherlands, and Sweden alone would encompass all of the countries that supply state-the-art PECVD systems, ion implanters, plasma dry-etchers, and lithography systems. Collective restrictions on exports to China should be established for key enabling equipment and technologies -- (1) for the manufacture of leading-edge dual-use (i.e. commercial and military application) ICs, and (2) for the R&D and design of advanced ICs and their technologies. In light of the difficulty the United States has encountered in achieving consensus with its allies in the past, it is recognized that achieving such agreements may

require elevation of this issue as a U.S. priority and where necessary, the application of leverage, including linkage with other bilateral issues.

- A similar bilateral agreement or understanding should be concluded with Taiwan.
- The Department of Commerce should be given a mandate and resources to compile an up-to-date catalogue of the global availability (including foreign availability) of state-of-the-art SME and design tools in designated foreign countries, particularly China. This catalogue should include, when necessary, classified information.

RECOMMENDATION 7 – SUSTAIN LEADERSHIP IN "STANDARD" PROGRAMMABLE MICROCHIPS

U.S. leadership in programmable standard microchips cannot be taken for granted, especially in light of the global consolidation underway in the semiconductor industry. Continued development of new programmable technologies is key to sustaining U.S. leadership. It is especially disconcerting that U.S. government research funding in this area has substantially decreased and that industry has focused on near-term research goals. Several technical areas affecting programmable standard product trustworthiness are important in RDT&E investment:

- Research on the Design of Programmable Elements. The DOD should partner with industry and with other government agencies, especially the NSF and Homeland Security, to fund university research that will ensure the domestic supply of scientists and engineers who are skilled in the development and use of programmable hardware.
- Best Practices. The DOD, in collaboration with other agencies such as NIST and with universities, and building on countertamper techniques developed in accordance with recommendation 9, should foster

the voluntary exchange of best practices for assuring trust of standard programmable hardware among commercial semiconductor developers, through the creation of courseware and industry information exchange programs. Developers of high-volume, standard parts are commercially motivated to ensure the integrity of their designs, both during the design and manufacturing process and once they are in operation. However, these suppliers are not well-informed of the means by which adversaries might attempt to compromise their designs and mechanisms that could be used to detect and deter such efforts. It is likely that a substantial improvement in the trustworthiness of standard commercial parts could be obtained simply through increased awareness of threat models and the exchange of best practices among the commercial parties.

- Research to Enable Firmware Integrity. A targeted DOD program in the area of firmware integrity would likely lead to the rapid development, dissemination, and adoption of improvements to these trust-related aspects of programmable parts. Today's standard parts, especially FPGAs, offer limited protection against the compromise of their firmware, i.e., the configuration software that is loaded into the parts prior to or during execution. The loading of low-level firmware (e.g., the BIOS) into CPUs can also have similar vulnerabilities. However, it is likely that suppliers of commercial parts would incorporate protective measures if they were readily available. Thus, DOD investment in university research in this area could yield significant improvements in the trustworthiness of standard parts.
- "Design for Trust Evaluation." In conjunction with the above, the DOD should initiate a research program on "design for trust evaluation" along the

lines of prior successful efforts on "design for testability." As previously indicated, the designs of modern programmable components are especially intricate, making it currently unfeasible to evaluate their trustworthiness. However, these complexities also plague chip verification and validation, making it increasingly difficult to produce designs that work reliably – let alone ones that can be shown to be uncompromised. DOD support for new approaches that simplify both validation and trust evaluation would be good candidates for commercial suppliers' further investment and adoption.

RECOMMENDATION 8 – SUPPORT DOD-UNIQUE TECHNOLOGY RESEARCH AND DEVELOPMENT

DOD must continue to support research and development of the special technologies it requires. This research and development includes ongoing radiation-hardened and EMP-resistant component design and process development; however, the emergence of requirements for trustworthiness requires new efforts in technologies to embed, assure, and protect component trust. The department will require additional technology development efforts. The task force suggests that DOD technology development balance be reexamined:

- Consider Reducing Barriers to Radiation-Tolerant "Standard" Designs. New generations of semiconductor processes may be inherently more tolerant to radiation than those of the past. However, export controls discourage commercial entities from studying and/or testing for these properties, let alone incorporating them into their "standard" parts. Similarly, future computer architectures may incorporate checkpoint/recovery mechanisms. Although these mechanisms are intended for the purposes of improved transaction performance and/or speculative processing, it is conceivable that they could also be used to recover

from transient events. However, commercial entities are reluctant to investigate or enhance these possibilities for fear that it would subject their designs to export controls. Export control policies should be reexamined to determine the right balance between increasing the suitability of standard parts to certain applications versus increasing the number of potential adversaries capable of mounting new challenges to U.S. interests through the availability of such parts. Loosening radiation-tolerance restrictions, for example, would result in future standard parts that could be used in military systems, easing requirements for radiation-hardened ASICs. The task force does not, however advocate easing export restrictions on radiation-hardened components.

- Increase Efforts to Develop Tamper Protection Technology. Once components have been proven trustworthy, antitamper protection is essential to protect chips from subversion or reverse engineering. The ongoing contest between adversary tamper efforts and U.S. defensive efforts in chip protection requires a continuous program seeking ever better ways to protect chip integrity.
- Develop Design and Production Techniques for Disguising the True Function of ICs. There may be future instances in which use of untrusted foundries is unavoidable. In those instances, camouflage offers one possible protection against subversion. The complexity of today's ICs offers the option of burying the true function of design in a sea of confusing logic.

RECOMMENDATION 9 – ENHANCE U.S. COUNTERTAMPER PROFICIENCY

Accurate characterization and assessment of adversaries' "dirty tricks" is essential to develop an effective U.S. countertamper strategy. The task force addressed many of these issues relative to the security challenges of information sharing, but opportunities, methods, and threats change continuously. The DDR&E, in conjunction with the intelligence community, should develop risk-mitigating technical approaches to support the risk management function. DDR&E should take the lead in defining the requirements and making the necessary investments to realize the needed security breakthroughs.

Specific actions needed to enhance U.S. countertamper proficiency include the following:

- The intelligence community should be tasked to
  - Characterize (through collection, analysis, and reporting) the capabilities and intent of key potential adversaries to subvert U.S. microelectronics. With this new insight, DDR&E should support development of techniques to detect subversions, attribute the subversions to an opponent, and establish consequences sufficient to deter the adversary's behavior. Detailed knowledge of likely adversary techniques allows focus on likely subversion means, increasing the effectiveness of tamper detection efforts.
  - Develop and keep current a catalog of subversive techniques for altering the behavior of microelectronic component design and implementation.

  - Establish current best practices for detecting and preventing subversive techniques, keeping in mind cost, both in money and time.[42]

- An investment strategy for enhancing U.S. countertamper evaluation capabilities should be developed. Current and projected capabilities must be highly protected; insight into U.S. detection abilities allows an adversary to tailor offensive approaches to reduce their cost and operational uncertainty.
- Establish an aggressive national antitamper development and evaluation program. Once the appropriate level of trust is established for a given component, effective, manufacturable, and affordable antitamper technology must be applied to the component to ensure the maintenance of trust.
- Initiate an annual competition to exercise the defensive approaches outlined above. This competition will provide estimates of the effectiveness of defensive techniques and increase confidence in the risk management process.
- Assess the subversion vulnerabilities of FPGAs. The innovative application of FPGAs in DOD critical systems shows great promise. However, aggressive adversarial analysis of these approaches has not been initiated.

A strategy for achieving the above hardware countertamper objectives without a comparable strategy for software is of limited utility. The task force recommends DDR&E

- Commission a similar DSB study to investigate national security issues associated with rapid

42. These items are recommended tasks for the IC.

migration of software production, testing, and maintenance overseas.

- Develop a national security strategy with corresponding implementation plan that couples the recommendations of the microelectronic and software studies and ensures that they are in balance and mutually supportive.

This page intentionally left blank.

APPENDIX A. TERMS OF REFERENCE

This page intentionally left blank.

THE UNDER SECRETARY OF DEFENSE
3010 DEFENSE PENTAGON
WASHINGTON, DC 20301-3010

ACQUISITION,
TECHNOLOGY
AND LOGISTICS

DEC 18 2003

MEMORANDUM FOR CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT: Terms of Reference -- Defense Science Board Task Force on High Performance Microchip Supply

You are requested to form a Defense Science Board Task Force on High Performance Microchip Supply.

The migration of semiconductor manufacturing and design capability to foreign countries imposes significant challenges upon the United States. The movement of manufacturing capability may leave the Department of Defense without an assured supply or access to emerging new designs. Failure to assure supplies may lead to future critical parts shortages at inopportune times, an inability to access new microchip designs in a timely manner during the design of new systems, or compromise sensitive national security information embedded in chip designs. In addition, the offshore movement of manufacturing and design capability could lead to inability to assure design function. The failure to assure design function could result in the intentional insertion of unknown vulnerabilities into vital pieces of equipment and result in the exploitation by a foreign government. A careful analysis of the implications associated with the movement to offshore manufacturing and design facilities is warranted.

The Task Force should assess the implications of the movement of manufacturing capability and design for three scenarios. As a minimum, the Department of Defense needs to address their ability to obtain radiation hardened microchips, the ability to produce limited quantities of special purpose microchips in a timely and secure manner, and the ability to produce microchips in a timely manner to meet emerging needs.

While investigating these scenarios the Task Force should address the following:

a. What are the root causes associated with the migration of the manufacturing capability of high performance semiconductors? Are there policies or technology investments that DoD, either alone or in conjunction with other US government agencies, can pursue which will influence the migration of manufacturing to foreign shores?

b. Do alternatives to the creation of trusted foundries based on US territory exist? Is testing a viable alternative and if so, what level of assurance will testing provide to guarantee that only intended functions are built into the microchip?

c. Are there alternative manufacturing techniques which will allow overseas fabrication of the microchips and subsequent interconnect development in the US? Can field programmable gate array (FPGA) microchips provide suitable performance capabilities for DoD's specialized needs?

d. Finally, are there future technologies which the US may invest in to replace the current microchip technology?

The Study will be co-sponsored by me as the Acting Under Secretary of Defense (Acquisition, Technology, and Logistics), the Director, Defense Research and Engineering, the Deputy Under Secretary of Defense (Industrial Policy), and the Assistant Secretary of Defense (Networks and Information Integration). Dr. William Howard will serve as the Task Force chairman. Dr. Chuck Byvik will serve as Executive Secretary and LTC Scott Dolgoff, USA, will serve as the Defense Science Board Secretariat representative.

The Task Force will operate in accordance with the provisions of P.L. 92-463, the "Federal Advisory Committee Act," and DoD Directive 5105.4, the "DoD Federal Advisory Committee Management Program." It is not anticipated that this Task Force will need to go into any "particular matters" within the meaning of Section 208 of Title 18, United States Code, nor will it cause any member to be placed in the position of acting as a procurement official.

Michael W. Wynne
Acting

APPENDIX B. TASK FORCE MEMBERSHIP

CHAIRMAN

Name	Affiliation
Dr. William Howard	Consultant

TASK FORCE MEMBERS

Mr. Bill Bandy	Matrics, Inc.
Mr. Steven Betza	Lockheed Martin
Ms. Christine Fisher	Consultant
Mr. Jim Gosler	Sandia National Laboratories
Mr. Tom Hart	Quicklogic Corporation
Dr. Thomas Hartwick	Consultant
Mr. Thomas Howell	Dewey Ballantine
Mr. Travis Marshall	Consultant
Dr. David Tennenhouse	Intel Corporation
Dr. James Van Tassel	Consultant
Mr. Owen Wormser	C3I

EXECUTIVE SECRETARY

Dr. Chuck Byvik	ODUSD (S&T)

DSB REPRESENTATIVE

LTC Scott Dolgoff	DSB OUSD (AT&L)

GOVERNMENT ADVISORS

Dr. Gerald Borsuk	NRL
Dr. Charles Cerny	AFRL/SNDM
Maj Anne Clark, USAF	DTRA
Mr. Dave Emily	NAVSEA, Crane Division
Dr. Barry Hannah	Navy Strategic Systems
Mr. Robert Jones	Space and Sensor Technology

Mr. Joe Keogh	U.S. Government
Dr. John Kosinki	US Army RDECOM CERDEC
Mr. Ray Price	NSA
Mr. Richard Ridgley	NRO
Mr. Mark Thompson	CIA
Mr. Steven VanDyk	Navy, Strategic Programs Office
LtCol Chris Warack	ODUSD(IP)
CDR John Zimmerman	ODUSD(IP)
Dr. John Zolper	DARPA

STAFF

Mr. Joe Maniaci	Strategic Analysis, Inc.

APPENDIX C. DEPUTY SECRETARY OF DEFENSE MEMO

This page intentionally left blank.

DEPUTY SECRETARY OF DEFENSE
1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010

OCT 10 2003

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTOR, PROGRAM ANALYSIS AND EVALUATION
DIRECTOR, NET ASSESSMENT
DIRECTOR, FORCE TRANSFORMATION
DIRECTORS OF DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Defense Trusted Integrated Circuit Strategy

The country needs a defense industrial base that includes leading edge, trusted commercial suppliers for critical integrated circuits used in sensitive defense weapons, intelligence and communication systems. The purpose of this memo is to establish a strategy to ensure that such suppliers exist. The strategy has five components:

a. Facilities Identification: Identify within the integrated circuit (IC) defense industrial base those facilities that could qualify as "trusted sources" for application specific integrated circuits (ASICs) based upon special facility clearances or other government agency technical certification. This survey will identify potential sources for the production of ASICs and will assess whether sufficient capacity currently exists to supply the defense and intelligence communities requirements on a competitive basis.

b. Product Identification: Identify the products that the above facilities can produce.

U16619 /03

c. Near term solutions: Using data identified in (a) and (b) above, identify and adjust acquisition strategies to maximize competitive opportunities while preserving domestic capability.

d. Research Initiatives: (1) Fund research to design and test procedures to assure security concerns have been met. (2) Fund research into next generation IC design for specialized defense applications.

e. Healthy Commercial IC Industry: We should ensure the economic viability of domestic IC sources. The health of the defense IC supplier community depends on the health of the larger commercial IC base. One important enabler of the larger commercial base is balanced policies that do not unnecessarily restrict US sources from the global economic market. Therefore, the DoD will support policies that provide a level playing field internationally for the procurement of commercial products.

Each part of the strategy will require detailed implementation plans. Because of near-term urgency, the Intelligence Community and DoD, using the NSA Information Assurance Directorate as Executive Agent, are taking actions to preserve a current domestic supply source.

Mr. Michael W. Wynne, Acting Under Secretary of Defense (Acquisition, Technology and Logistics), will oversee implementation of the strategy. He will coordinate responses to any inquiries about integrated circuits or semiconductors. Miss Suzanne Patrick, Deputy Under Secretary of Defense for Industrial Policy; Dr. Charles Holland, Deputy Under Secretary of Defense for Science and Technology; and Mr Robert Lentz, Director, Information Assurance, Office of the Assistant Secretary of Defense for Networks and Information Integration will coordinate implementation of the strategy. Their action officer is Lieutenant Colonel Chris Warack, USAF. You may reach him by telephone at (703) 602-4323 or by electronic mail at christopher.warack@osd.mil.



APPENDIX D. FUTURE TECHNOLOGY DEVELOPMENT

The Department needs to secure continued "Moore's Law" improvements in processing capacity that will enable it to maximize the advantages inherent in its superior sources of information and the superiority of the algorithms and networks that are used to process and benefit from them. Even a "level playing field" in which "standard" programmable microchips of ever increasing capacity are available to both the DOD and its adversaries works to U.S. advantage, especially if the suppliers of those parts are U.S. based. In contrast, if the microchips available are not powerful enough to take full advantage of superior sensor, actuator, algorithm, networking and systems capabilities, U.S. superiority will rapidly erode.

Historically, the rapid rate of growth in U.S. microchip capability resulted from a robust national portfolio of long-term research that incorporated both incremental and revolutionary components. Industry excelled in evolutionary technology developments that resulted in reduced costs, higher quality and reliability and vastly improved performance. DOD now is no longer perceived as being seriously involved in – or even taking steps to ensure that others are conducting – research to enable the embedded processing proficiency on which its strategic advantage depends. This withdrawal has created a vacuum where no part of the U.S. government is able to exert leadership, especially with respect to the revolutionary component of the research portfolio. [43] The problem, for DOD, the IT

43. This development is partly explained by historic circumstances. Since World War II, the DOD has been the primary supporter of research in university Electrical Engineering and Computer Science (EECS) departments, with NSF contributing some funds towards basic research. From the early 1960's through the 1980's, one tremendously successful aspect of the DOD's funding in the information technology space came from DARPA's unique approach to the funding of Applied Research (6.2 funding), which hybridized university and industry research through a process that envisioned revolutionary new capabilities, identified barriers to their realization, focused the best minds in the field on new approaches to overcome those barriers and fostered rapid commercialization and DOD adoption. The hybridization of university and industry researchers was a crucial element; it kept the best and the brightest in the

industry and the nation as a whole, is that no effective leadership structure has been substituted. Instead, research in these fields is managed through a hodge-podge of programs spawning numerous government agencies. The President's budget includes "cross-cuts" of the government's Nanotechnology (the NNI) and IT (the NITRD) research investments, each of which is stitched together by committees representing the participating agencies. However, there is no unified source of leadership that can mount revolutionary programs, let alone ensure that the DOD's future requirements for programmable microchips will be met.

While it is tempting to believe that the future capabilities DOD will require will emerge solely from the private sector, most commercial entities can only engage in relatively short-term incremental R&D on their own. Although the industry has pooled its resources to support a limited degree of long-term university research (e.g., through the SRC), this is far from sufficient to meet DOD's needs. Similarly, it may be tempting to believe that NSF funding will be sufficient to sustain information superiority. Although NSF funding has risen and the NSF does fund more longer term incremental work than industry, the NSF does not typically support development of revolutionary capabilities, along the lines of those achieved by DARPA's 6.2 programs.

---

university sector well informed of defense issues and the university researchers acted as useful "prods" to the defense contractors, making it impossible for them to dismiss revolutionary concepts whose feasibility was demonstrated by university-based 6.2 efforts that produced convincing "proof of concept" prototypes. As EECS grew in scale and its scope extended beyond DOD applications, a "success disaster" ensued in that EECS essentially "outgrew" the ability of the DOD to be its primary source of directional influence, let alone funding. Furthermore, DOD never developed a strategy to deal with this transition. With pressures to fund developments are unique to the Defense (e.g., military aircraft, tanks, artillery, etc.), the DOD withdrew its EECS research leadership. Recently, DARPA has further limited university participation, especially as prime contractors, in its Computer Science 6.2 programs, which were by far its most significant investments in university research (vastly outstripping 6.1 funding). These limitations have come in a number of ways, including non-fiscal limitations, such as the classification of work in areas that were previously unclassified, precluding university submission as prime contractors on certain solicitations, and reducing the periods of performance to 18-24 months.

Past investments in research would appear to secure Moore's Law scaling through 2009 or 2011. However, beyond that, the microchip industry faces three key challenges, each of which puts DOD's information superiority at risk, but also poses opportunities for DOD to tilt the economics of non-standard (e.g., low volume) microchip manufacturing in its favor:

- There is a significant technology gap in the 2013-2019 time frame, as transistor critical dimensions shrink below 10-12 nm. While the continued use of charge-based devices (devices based on the movement of electrons) remains feasible during this period, there is an urgent need for revolutionary approaches to development new operating principles and materials for use in those devices. Surprisingly, very little of the U.S. government's National Nanotechnology Initiative (NNI) is addressing this issue – yet the window for the timely conduct and insertion of such research is rapidly closing. The need for new technologies for use in ten years may also present an opportunity to contain the capital costs associated with microchip manufacturing. For example, one alternative that has been suggested involves the use of chemical processes to create nano-wire / nano-dot devices in bulk and to use self-assembly techniques to create small clusters of "pre-wired" devices and precisely position them on a microchip substrate. Taking this line of reasoning a step further, it may be possible to use what would then be "legacy" 10-20 nm lithography technology to wire together these self-assembled clusters. Since the "legacy" lithography and associated mask-making equipment would by then have been substantially depreciated, the capital equipment costs associated with such a manufacturing approach might not be as prohibitive to the DOD as they are today. Direct imprint lithography is another alternative that is being

investigated, though its viability at the finest feature sizes remains uncertain.

- New approaches to the architecture of programmable microchips and to their programming concepts are required to extract benefit from the huge numbers of transistors made available by Moore's Law advances. The design of super-complex chips is being influenced by three transitions, each of which presents risks and opportunities. First, standard CPUs and DSPs are evolving from single core (i.e., processor) devices to multi-core devices.[44] Secondly, standard Programmable Gate Arrays (PGAs) are undergoing a transition in which PGA fabrics are combined on the same chip with CPUs and DSPs. This process, which is to the DOD's advantage, will likely intensify with the advent of multi-core processor architectures described above. Finally, the sustained use of sub-wavelength lithography over coming generations of transistors will push designers of complex logic towards regular transistor patterns. This may reduce the gap between PGAs and other forms of logic, further accelerating the combination of PGAs with many-core processors.
- In the early 2020's, thermal noise limitations suggest a need to transition beyond charge-coupled devices

44. Initially, this will be a relatively mild transition as the components of dual processor systems are integrated onto a single chip. However, as the number of cores scales up to hundreds and then thousands of cores per die, the impact of this transition will be far more pronounced. Going forward, the use of parallel independent computational elements (vs. frequency scaling, pipelining, etc.) will be the means of extracting increased performance from these microchips – not just for supercomputers, but for desktops, handhelds and embedded systems as well.. **Arguably, this is the computer industry's largest transition since the adoption of the microchip – and possibly since the invention of the stored program computer.** Key challenges arising from this transition have to do with: the on-chip networks interconnecting the cores; Memory and I/O bandwidth to feed these microchips; and the programming environments that will allow their capacity to be harnessed by large numbers of programmers / users.

to those based on other physical principles, such as spin. Since these new technologies are unlikely to instantaneously transition to high volume manufacturing, it is likely that there will be some period during which their economics could favor lower volume applications, presenting another opportunity for the DOD to re-assert leadership and gain strategic advantage. Conversely, ceding leadership in this transition to nations that are potential adversaries would certainly undermine our information superiority – and may also undermine a key economic component of our national security.

This page intentionally left blank.

APPENDIX E. VERIFYING CHIPS MADE OUTSIDE THE UNITED STATES

RANDY GOODALL, SEMATECH

Q2- Verifying Chips Made by Foreign Suppliers / Sites

- Unlikely to be verifiable by non-destructive testing
- Signal testing
  - Probably in the NP group of problems ("traveling salesman")
  - Hueristics likely, but what is good enough in advanced 21st century warfare?
- Measurement testing
  - Acoustic and high-energy photon imaging, mechanical (mass, moments of inertia, …)
  - Must have the resolution of devices/layers (nano somethings)
  - Non-complex wave analysis is non-deterministic
  - Isomorphic to the intractable wafer (or reticle) inspection problem, but with HUGE signal-to-noise ratio due to intervening medium of package and/or upper layers
    - Unpackaged is only a little better proposition
- What cost penalty is allowed?
  - Comparison to building/upgrading a small fab?

SEMATECH Briefing to DSB- June 23, 2004 • Slide 23

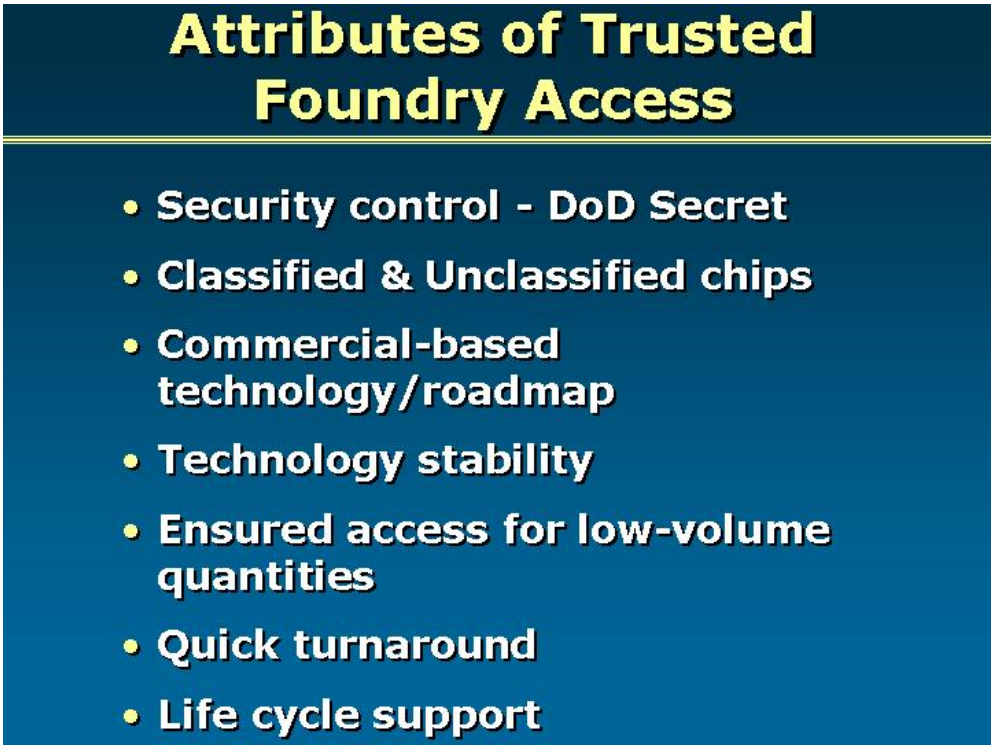
This page intentionally left blank.

APPENDIX F. TRUSTED FOUNDRY PROGRAM



This is the first component of the Trusted Foundry Access Program[45]. This contract was established to provide a trusted foundry to cover leading edge requirements. There are on-going activities to expand the number of trusted foundry sources to cover all technology needs.

45. Extract from presentation given to the Task Force by Chuck Varney, NSA

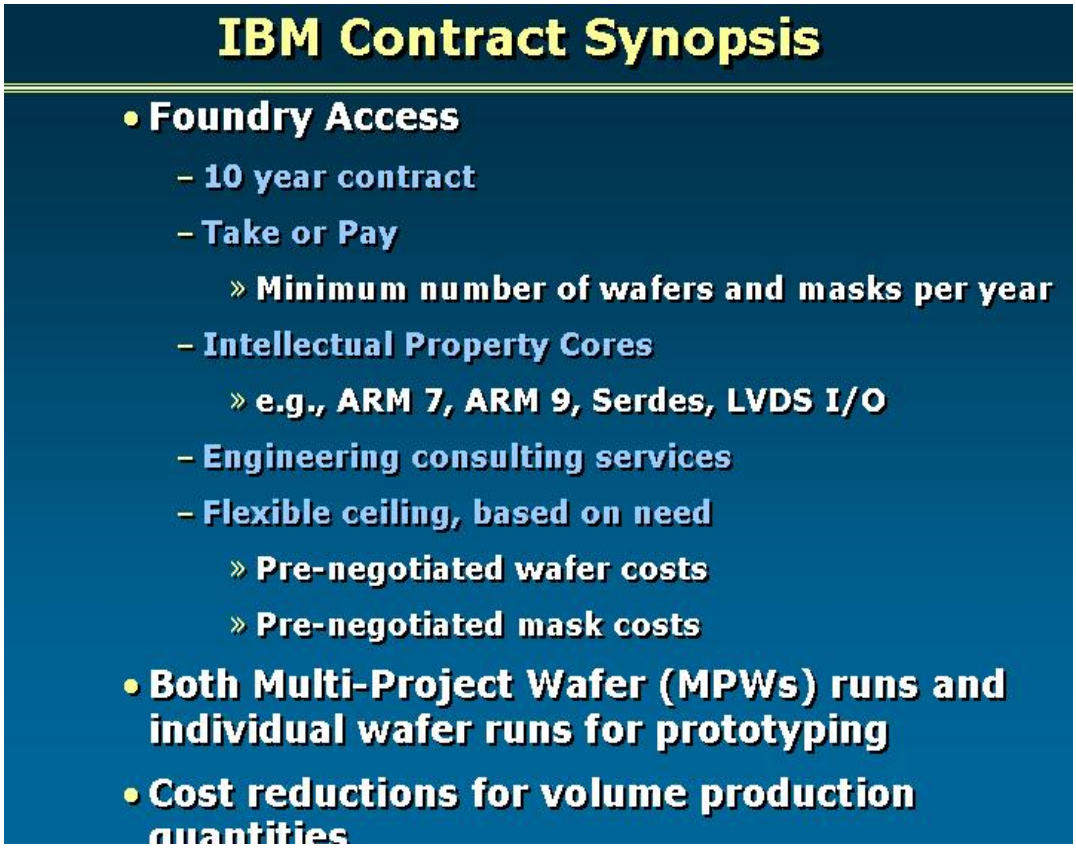


Security controls allow for clearance of personnel necessary to protect the product at a maximum of DOD Secret. The number of people necessary is dependent on the automation of the plant - the more fully automated, the fewer people necessary.

Trusted parts imply that accountability controls have been imposed to guarantee that the parts were manufactured as expected, whether they were classified or unclassified. Classified parts would also have the same controls imposed on their manufacture.

Accelerated turnaround times are available; however, this should be pre-coordinated with the foundry. A certain number of accelerated turns have been pre-paid, additional ones can be purchased.

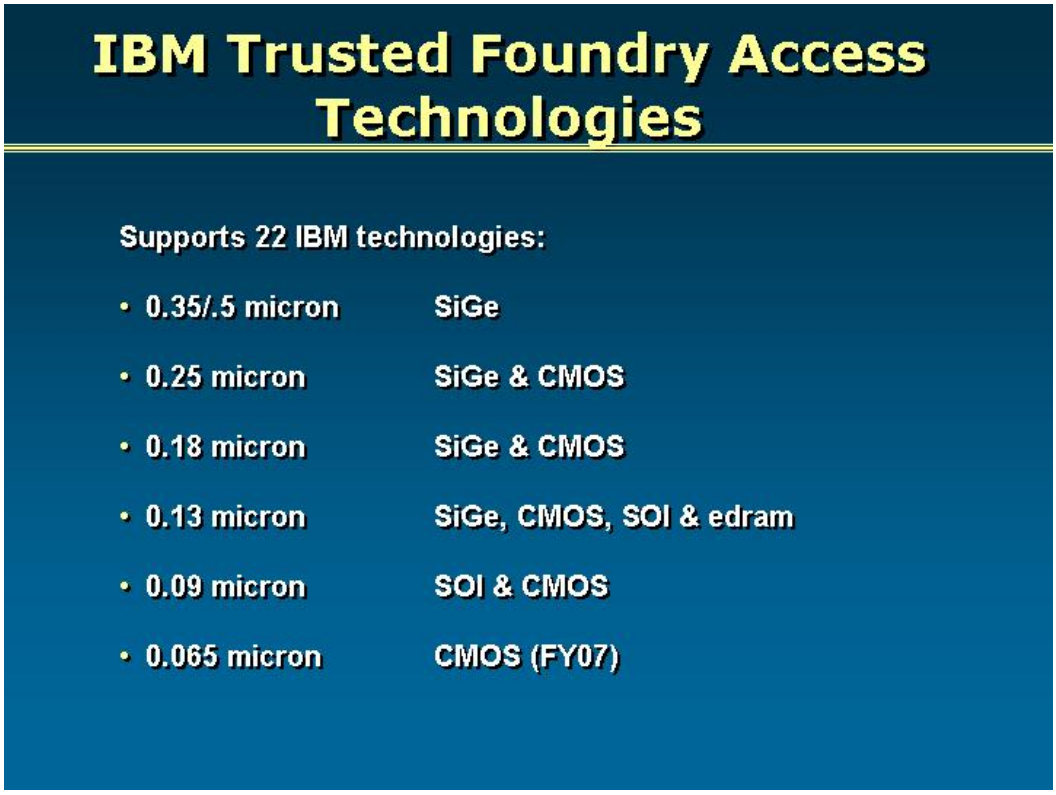
Life cycle for the processes is based on the commercial viability of the process. Typical processes will last 10 years. In addition, the foundry will provide a 2 year notification for any of the processes they plan to retire. All programs that have ordered parts with that process will be notified in order to provide them the opportunity to order an end-of-life buy.



The contract lasts for up to 10 years, with the government having the option to re-new the contract each fiscal year.

The contractual amount is set for each year and is comprised of prototype runs (mask set + half lot expedited run), production runs, and Intellectual Property licensed design drop-ins. There is the provision to trade between these areas, keeping the overall contract amount fixed.

This is a take or pay contract. The contract provides pre-paid foundry access to government programs. The foundry will provide access; however, if the government doesn't order all the parts that they have access to for any fiscal year, they will lose that remaining access for that year.



The processes are priced based on their complexity. SiGe runs will cost more than CMOS runs, and processes will become more costly as the geometry becomes smaller. However, the costs also are adjusted (usually lowered) each year to compensate for access to an older technology.

APPENDIX G. COMPARISON OF ASIC AND FPGA SYSTEM CHARACTERISTICS

ASIC vs FPGA Tradeoffs

ASIC IMPLEMENTATION ISSUES	*FIELD PROG. GATE ARRAY**	*MASK PROG. GATE ARRAY*	*STANDARD CELL ARRAY*	*FULL CUSTOM*
Power Dissipation	2- 10	2	1.5	1
Utilization of Available Transistors	0.1 - 0.9	0.7	1	1
Signal Processing Performance	0.1 - 0.5	0.5	0.8	1
Typical Hardware Fabrication Time	1	4	16	16
Fabrication Cost	1	2	7	7
Physical Size	4	2	1.5	1
Available Sizes	Limited	Limited	No Limit	No Limit
Ability To Upgrade After Put Into Use	Yes	No	No	No
Availability Of Components For Mixed -Signal Design	Limited	Limited	Limited	Yes
Ability To Isolate "Red"/"Black" Regions	No	Limited	Yes	Yes
Flexibility Of I/O Protocols	Limited	Yes	Yes	Yes

Numbers are Normalized, Where 1 is the Optimum

*** Range Provided for FPGAs Because Some Applications use FPGA Real Estate and Components More Efficiently Than Others**

Source: Mayo Clinic

MAYO CLINIC SPPDG

Example of tradeoffs ASIC vs FPGAs for a Space System

Parameter	ASIC	FPGA
Weight (lbs)	260	412
Power (W)	2600	4200
Development time (months)	27	5
Cost (NRE)	$30M	$1.5M
Clock speed (MHz)	180	210
Technology (um)	.18	.13
# of gates (Millions)	7.1	8
# of boards	20	40
Design reusability	Low	High

Source: Lockheed Martin

This page intentionally left blank.

APPENDIX H. DFAR SUPPLEMENT

DEFENSE FEDERAL ACQUISITION REGULATION SUPPLEMENT

Proposed

(xxx.yyy-zzzz) Restriction on Acquisition of Application Specific Integrated Circuits

1. Definitions. As used in this clause—
    a. 'Application Specific Integrated Circuit' or 'ASIC' means any custom microelectronics device (digital or mixed-mode digital/analog) that is fabricated at a semiconductor foundry, including fully custom integrated circuits and gate array class devices.
    b. 'Trusted Foundry' means a semiconductor manufacturing facility that has been certified by the DOD to provide secure semiconductor fabrication and data management, including the capability for fabricating classified ASIC designs.

2. Except as provided in paragraph (c) of this clause, all Application Specific Integrated Circuits delivered under this contract, either as end items or components of end items, shall be wholly fabricated and manufactured at a Trusted Foundry in the United States.

3. The restriction under paragraph (b) of this clause does not apply to—
    c. Commercial-off-the-shelf microelectronic devices that are procured via standard part numbers and are not modified at the manufacturer for DOD use.
    d. Field Programmable Gate Array devices that are procured via standard part numbers and are later personalized at DOD laboratories or Contractor facilities.

e. Custom microelectronic devices that are analog in nature (e.g. radio frequency amplifiers, custom analog hybrids) that do not contain any digital logic.

4. The restriction in paragraph (b) of this clause may be waived upon request from the Contractor in accordance with subsection 225.7009-3 of the Defense Federal Acquisition Regulation Supplement. The Contractor must provide compelling rationale for waiver of this restriction, and the waiver must be approved in writing by the DOD Trusted Foundry Program Office.

5. The Contractor shall retain records showing compliance with the restriction in paragraph (b) of this clause until 3 years after final payment and shall make the records available upon request of the Contracting Officer.

6. The Contractor shall insert this clause, including this paragraph (f) in all subcontracts, except those for—
   f. Commercial items other than Application Specific Integrated Circuits; or
   g. Items that do not contain Application Specific Integrated Circuits

APPENDIX I. MINORITY REPORT

Essential portions of this report with which I heartily concur are the pressing need for greater chip security, continued future supply guarantees via a trusted foundry, and acquisition reform to lay the foundation for a stronger DOD infrastructure. My dissent takes issue with the depth of analysis of the data this committee received and the recommendations relating to the semiconductor industry. In my view, aspects relating to financial support of semiconductor industry activities, especially extraordinary DOD support, are not supported by business strategies and logic based on this committee's investigation. To be more blunt, it is not DOD's job to re-vamp the infrastructure of this healthy, robust and very profitable industry, rather, DOD interest's have to be evaluated in a cost benefit analysis such as DARPA routinely performs based on the DOD mission. Our nation would be better served if government provided the catalyst or leadership (non-financial support), apparently missing in the semiconductor industry, to facilitate a better semiconductor industry long term strategic plan.

Dr. Thomas Hartwick
Defense Science Board High Performance
Microchip Supply Task Force Member

This page intentionally left blank.

APPENDIX J. ACRONYMS

AFOSR	Air Force Office of Scientific Research
AGED	Advisory Group on Electron Devices
AMD	Advanced Micro Devices Inc.
ARO	Army Research Office
ASIC	Application Specific Integrated Circuit
BIOS	Basic Input Output System
CFIUS	Committee on Foreign Investments in the United States
CMOS	Complimentary Metal Oxide Semiconductor
COTs	Commercial off the Shelf
CPLD	Complex Programmable Logic Devices
CPU	Central Processing Units
DARPA	Defense Advanced Research Projects Agency
DCMA	Defense Control Management Agency
DDR&E	Director of Defense Research and Engineering
DEPSECDEF	Deputy Secretary of Defense
DOD	Department of Defense
DoE	Department of Energy
DoS	Department of State
DoT	Department of Transportation
DRAM	Dynamic Random Access Memory
DSB	Defense Science Board
DTIC	Defense Technical Information Center
DTICS	Defense Trusted Integrated Circuits Strategy
DTRA	Defense Threat Reduction Agency
DUSD	Deputy Under Secretary of Defense
DUSD(IP)	Deputy Under Secretary of Defense for Industrial Policy
EMP	Electro Magnetic Pulse
EU	European Union
FPGA	Field Programmable Gate Array
GBI	Ground Based Interceptor
GFE	Government Furnished Equipment
IBM	International Business Machines Inc.
IC	Integrated Circuit

IDA	Institute for Defense Analyses
IP	Intellectual Property
IPT	Integrated Product Team
ITAR	International Traffic in Arms Regulations
JTRS	Joint Tactical Radio System
KIET	Korean Institute of Electronics Technology
M1A1	Abrams Main Battle Tank
MIT	Massachusetts Institute of Technology
MMST	Microelectronics Manufacturing Science and Technology
MPU	MicroProcessor Unit
NDIA	National Defense Industries Association
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSC	National Security Council
NSF	National Science Foundation
ODUSD (IP)	Office of the Deputy Under Secretary of Defense for Industrial Policy
ONR	Office of Navel Research
OSD	Office of the Secretary of Defense
PECVD	Plasma Enhanced Chemical Vapor Deposition
PLA	Programmable Logic Array
PLD	Programmable Logic Device
RDT&E	Research Development, Test and Evaluation
RHMATD	Radiation Hardened Microelectronics Accelerated Technology Development
RHOC	Radiation Hardened Oversight Council
RISC	Reduced Instruction Set Computer
S&T	Science and Technology
SAR	Synthetic Aperture Radar
SDD	System Design and Development
SIA	Semiconductor Industry Association
SME	Semiconductor Manufacturing Equipment
SOC	System on Chip
SPO	System Program Office
SRAM	Static Random Access Memory
TI	Texas Instruments Corporation
TSMC	Taiwan Semiconductor Manufacturing Company

UCLA	University of California Los Angeles
UMC	United Microelectronics Corporation
USD(ATL)	Undersecretary of Defense for Acquisition, Technology, and Logistics
USTR	United States Trade Representatives
VAT	Value Added Tax
WTO	World Trade Organization