Statement of Dr. Brian S. Cohen
Institute for Defense Analyses
Assistant Director, Information Technology and Systems Division
On
Integrated Circuits Supply Chain Issues in a Global Commercial Market – Defense Security and Access Concerns
Before the
House Armed Services Subcommittee
Terrorism, Unconventional Threats and Capabilities

March 14, 2007

Mr. Chairman and distinguished members of the Subcommittee, I am pleased to speak to you today about efforts to mitigate potential national security concerns resulting from the off-shore migration to major elements of the Integrated Circuit (IC) industry. I have spent much of my career at the Institute for Defense Analyses (IDA) working to help Department of Defense (DOD) understand and assess the emergence of what is now clearly a global IC market dominated by commercial interests and supplied by what is frequently a non-U.S. industry base. In 2002, I started work on DOD efforts to deal with concerns about the declining domestic sources of ICs and consequent increased dependence on foreign sources for critical ICs. Much of this work focused on the Trusted Foundry Program and the accreditation of Trusted Suppliers, particularly for custom-designed ICs[1]. While more work is required to find solutions for all types of ICs and for the broader elements in the supply chain, the Department has had considerable success in using the Trusted Foundry and Accredited Trusted Suppliers for custom-designed ICs. My statement today addresses this work.

Background

The information revolution in the recent past has had a profound effect on DOD. Looking back over the last fifty years, there are two clear technical pillars for the information revolution, microelectronics, as exemplified by ICs, and information technology (IT). The synergistic emergence of these areas has fueled dramatic innovation. DOD had an important and leading role in the development of the technologies and industrial base for both microelectronics and IT and without them key DOD strategies such as network-centric warfare would not be possible. Nevertheless, here we are today, struggling with change in both of these areas. A few decades ago both the microelectronic IC and IT industries had major market segments in Defense, but both have become primarily commercial. These days the DOD market, even taken in its entirety, is today a small customer for the IC industry.[2] Defense performance and operating

[1] Also called Application Specific Integrated Circuits (ASICs).

[2] A general rule of thumb is that a fabrication plant requires 3X its capitalization in annual revenue to make business sense. For a $5 billion plant this is $15 billion in annual revenue. IDA estimates that DOD (through its suppliers) purchases about $1 billion annually in military/aerospace ICs, and perhaps $2-4 billion annually of additional commercial ICs. While a detailed census is difficult to obtain, there seems to be no business case for a captive defense state-of-the-art fabrication.

environment requirements can differ from commercial needs and are often sensitive from a security perspective. Captive DOD IC capabilities are very expensive and difficult to keep at the leading edge, so DOD struggles with how their specialized needs can be met by commercial-focused sources. A recent Defense Science Board[3] examined these issues and some recommended actions. The report, while recognizing that the domestic IC industry was being driven offshore primarily by commercial factors, suggested that a long-term solution would be to establish domestic IC competitiveness as a national priority.

What are the Defense Security and Access Concerns?

ICs are extensively used in DOD computing, communications, and sensors. Most of these ICs are catalog, off-the-shelf items, such as processors and memories. However, some IC applications require specialized functions and/or have unique military performance demands. Such ICs are custom-designed and manufactured. Custom-designed ICs are generally the most security and access sensitive ICs in defense systems, as they may contain key intellectual property (such as algorithms) and because their proper functioning may be the crucial element in system performance. These custom-designed ICs are also more easily targeted by adversaries as they are tested by a relatively small user base for use in a limited number of applications. On the other hand, for memory ICs that are widely used by millions in the civilian sector, successful targeting and modification of such a commodity product is more difficult.

The primary national security concerns related to ICs are:

- Theft of important intellectual property such as algorithms encoded as part of the chip design
- Tampering with IC function thereby potentially causing defense systems to be ineffective, unavailable, or to allow unauthorized access
- Denial of access to advanced technologies and supplies, resulting in only older ICs being available for defense use

One might ask whether it is actually feasible that an adversary might steal intellectual property or tamper with defense supplies. To perform these nefarious acts, an adversary (whether nation state or individual actor) needs to:

- Perceive some benefit from the exploitation (motivation)
- Have the capability to perform the exploitation (capability)
- Have the opportunity to perform the exploitation (vulnerability)
- Have confidence of success (ability to target/avoid detection)

Although I cannot describe the details of the threats, vulnerabilities and capabilities in this forum, IDA studies and analyses have identified plausible instances where these threats to IC integrity are real.

One way of understanding an area like tampering is to look at counterfeiting which is a subset of tampering. The motivation for counterfeiting is usually monetary and the rate at which this

[3] *Defense Science Board Task Force On High Performance Microchip Supply*, February 2005, http://www.acq.osd.mil/dsb/reports/2005-02-HPMS_Report_Final.pdf.

problem is found in industry indicates that this is more than sufficient motivation.[4,5] Detected counterfeit ICs are usually found because they malfunction or are substandard,[6] but a good counterfeit or tampered IC may appear by any measure to be a good part. These seemingly good but counterfeit parts are not likely to be detected. The alarming thing about counterfeiting is that we assume that the motivation for the observed counterfeit is monetary, but that may not always be the case. The mere fact that counterfeit ICs have entered the defense supply chain and have been found (because of their failure), demonstrates the feasibility of a tampered part with malicious intent also being inserted into the supply chain.

Finally, it is important to highlight that custom-designed and custom-manufactured ICs constitute only a small portion of Defense IC purchases. Most ICs used in DOD systems are catalog items that are mass-produced and, although they are not as easily targeted, there are security and access concerns with these products. It is also important to note that while ICs are but one element of the supply chain, there are serious concerns about the loss of domestic capability in other areas of the supply chain. IC packaging and assembly have already moved off-shore, and it makes little sense to go to great lengths to obtain trusted ICs only to ship them to some foreign company for packaging and assembly. A recent report by the National Research Council highlighted concerns about the printed circuit board industry moving offshore[7]. The Department will need to consider security and access concerns for the entire supply chain.

Trusted Foundry and Accredited Trusted IC Suppliers

The Trusted Foundry Program, initiated in FY 2004, leverages a contract with IBM to aggregate purchases of leading edge (CMOS/SiGe 90nm – 130 nm currently) IC manufacturing technologies for use in defense applications. As required by contract, the contractor upgraded their facilities and implemented enhanced security procedures, creating the Department's first Accredited Trusted IC Supplier. The Office of the Secretary of Defense (OSD) tasked the National Security Agency (NSA) to stand up a new office to manage this contract and, in response, NSA created the Trusted Access Program Office (TAPO) to perform this function. OSD also requested that NSA expand the ranks of suppliers capable of providing trusted ICs, and NSA implemented the trusted IC supplier accreditation. Just to summarize the difference between these two efforts:

- Trusted Foundry – Aggregated DOD buying (through TAPO) of ICs manufactured by the Trusted Foundry contractor as an Accredited Trusted IC Supplier. TAPO assists in the aggregation of defense purchases.

---

[4] *Counterfeit parts nettle buyers, China seemingly unable to stem tide of bad components*, Electronics Supply and Manufacturing, 08/18/2003 (http://www.my-esm.com/showArticle.jhtml?articleID=13100410).

[5] *Bogus! Electronic Manufacturing and Consumers Confront a Rising Tide of Counterfeit Electronics*, M. Pecht and S. Tiku, IEEE Sprectrum, May 2006.

[6] Panther Electronics of Fort Lauderdale, FL, was indicted by a federal grand jury on charges related to the sale of parts used in radar and communication systems on several military aircraft. Panther is accused of selling more than 400 microcircuits and connectors to the Air Force and Navy for use on F-14, F-15, and B-1 bombers. Random testing by the Defense Department found that approximately 20 percent of the parts purchased were either non-conforming or counterfeit. (source, Defense Supply Center Columbus, DLA/DSCC).

[7] *Linkages: Manufacturing Trends in Electronics Interconnection Technology, Committee on Manufacturing Trends in Printed Circuit Technology*, National Research Council (2005) (http://books.nap.edu/catalog.php?record_id=11515).

- Accredited Trusted IC Supplier – Supplier that is accredited as meeting the Trusted Supplier criteria. Customers go directly to the supplier

It is important to note that while the Trusted Foundry Program was created to manufacture ICs, reengineering the business structure to aggregate provided purchases across programs. This aggregation of purchases is an important parallel innovation, which has resulted in a substantial improvement in access to advanced technologies and cost savings. Multi-project wafers[8] and sharing both the access fees and infrastructure allowed customers to achieve substantial savings.

The Trusted Foundry Program is funded through equal investments from DOD[9] and NSA as well as from direct program reimbursements for acquisitions. The DOD share was approximately $31.2 million in FY 2005 and rises to $40 million in out years. The TAPO has made significant efforts to connect customers with the Trusted Foundry Program and in FY 2006, more than $100 million in business was performed through the program.

As a business approach, IDA views the Trusted Foundry to be successful. To date, 26 program requirements have been fulfilled. In FY 2006, 13 multi-project wafers were assembled and manufactured with an average of 15 IC designs on each. TAPO estimates in excess of $160 million in savings over comparable spot prices.

IDA's work on the Trusted Foundry

In 2002, during a cyclical downturn in the IC industry, it appeared that most, if not all, new state-of-the-art IC fabrication plants were being planned for construction off-shore. IDA was asked by OSD to assist in responding to Congressional concerns about whether a captive foundry could address security issues and retain domestic control of the capability. We found that a captive domestic capability would be far from economical and would be challenged to achieve and sustain leading edge technologies. Our research further concluded that while the current business structure was low cost, it did not support key military needs or address security requirements. The IDA study recommended a restructured approach that called for cooperation with commercial industry. At the same time, NSA, looking at how to meet its needs for specific ICs, had identified a potential approach using a take-or-pay arrangement with a commercial (domestic) IC firm (IBM). This became the basis of the Trusted Foundry Program.

In February 2003, IDA was asked to evaluate a technical proposal from NSA and IBM. IDA' assessment was positive, but recommended that the endeavor be Defense-wide, rather than focused solely on NSA. Subsequently, the Department moved forward with the Trusted Foundry as a DOD-wide effort. The Trusted Foundry Access program office (subsequently renamed to the Trusted Access Program Office (TAPO)) was established at NSA in January 2004, providing initial guidance and immediately kicking off an effort to bring in additional suppliers. The initial

[8] Multi-project wafers (MPWs) take several integrated circuit designs and combine them onto a single manufacturing run, thereby distributing the significant non-recurring expenses. These savings can be significant. It is important to note that the TAPO manages the aggregation of customers into MPWs, although contractors actually will perform the final merger of the designs into a single manufacturing run. At this time, TAPO only aggregates for production through the Trusted Foundry.

[9] The DOD funding is from PE 0605140D8Z (http://www.dtic.mil/descriptivesum/Y2007/OSD/0605140D8Z.pdf).

guidance, (which remains in effect today) required that programs with high mission assurance requirements manufacture custom-designed ICs through a "trusted foundry service."[10]

In order to leverage and be harmonious with other efforts, the concepts of how to specify trust for IC suppliers is based on the ideas already established in the information/mission assurance area. The DOD policy[11] requires that custom-design ICs for high Mission Assurance Category (MAC)[12] and confidential environments be obtained from an Accredited Trusted IC Supplier.

In early 2005, IDA assisted TAPO with a survey of industry interest in trusted supplier accreditation. There was strong interest from industry, and subsequent efforts have resulted in 6 companies becoming accredited (including 2 Rad Hard and 1 Compound Semiconductor) with 8 more accreditations in process.

Since then, IDA has helped OSD to clarify the concepts and required policies. A summary of the key policy concepts was presented at GOMACTech-2006.[13] The recent focus of work has been on extending the concepts to cover a range of assurance requirements[14] (e.g., moderate assurance levels as well as high) and to address defense requirements for all types of ICs beyond custom-designed.

While Accredited Trusted IC Suppliers provide one element of defense, IDA has continued to examine a range of approaches to addressing the security and access concerns. IDA has recommended that the Department also consider techniques such as anonymity in acquisition, encryption of designs and authentication.

DARPA was an early participant in the Trusted Foundry Program and was interested in identifying research opportunities that could address the concerns of IC security. In August 2005, IDA held a workshop at the request of a DARPA Program Manager with the objective of exploring research opportunities that hold promise for revolutionary advances in protecting the security and integrity of the microelectronic chips, primarily for defense or National Security applications. A small group of experts were invited and various techniques and technologies were discussed that might protect against the theft of intellectual property on the chip or unauthorized modification of ICs. A broad portfolio of techniques was considered for addressing these two concerns, including digital watermarking, steganography, self-test, verification, validation, hardware/software co-implementation, and secured programmable gate array devices. Some classified techniques were also discussed such as design obfuscation, anti-tamper techniques, secured PKI, and design encryption.

---

[10] Initially "trusted foundry service" implied that the ICs needed to be manufactured through the Trusted Foundry, but today, this is interpreted as being provided by an Accredited Trusted IC Supplier.

[11] Under Secretary of Defense (ATL)/Assistant Secretary of Defense (NII) Memorandum, *Interim Guidance on Trusted Suppliers for Application Specific Integrated Circuits (ASICs)*, January 27, 2004.

[12] DOD Directive 8500.1, "Information Assurance," October 24, 2002, (http://www.dtic.mil/whs/directives/corres/pdf/850001_102402/850001p.pdf).

[13] *Perspectives on Defense Trusted Integrated Circuit Policy*, paper presented at Government Microelectronic Applications & Critical Technology (GOMACTech) Conference - 2006, Unclassified, March 2006

[14] The initial policy required that only high mission assurance required the use of the Trusted Foundry. Extension of the policy to define how to handle more modest mission assurance requirements is more challenging.

The Trusted Foundry and Broader Concerns

DOD depends strongly on global commercial sources for the majority of its IC purchases and many of these are likely to continue to come from foreign sources. These ICs are not likely be supplanted by either the Trusted Foundry or by Accredited Trusted IC Suppliers. The Trusted Foundry/Supplier, in its current form, is oriented towards addressing immediate security and access concerns by partnering with domestic suppliers. It has been successful partly by enabling industry to reap the benefits of a differentiated "trust" market, and in some cases a managed customer base. While the criteria for a domestic supplier to become trusted (i.e., cleared facility and personnel) is reasonably achievable and affordable, large foreign based commercial firms will not be able to readily clear their facilities and personnel.

Additional DOD initiatives are likely to be needed to address the broader or long-term problems, including the issues surrounding mass-produced ICs. Another challenge is to how to obtain ICs from foreign sources and have some level of assurance despite their coming from foreign sources. For commodity ICs, the vulnerabilities and affordable mitigating techniques are markedly different from the techniques appropriate for custom ICs. There are alternative practices, such as anonymous acquisition of ICs, which can protect the identity of the customer (i.e., defense program offices) and provide a reasonably effective and affordable approach.

In the long-term, in order to fully leverage the global commercial market for ICs, DOD will have to come to terms with some key research challenges:

- How can DOD trust (at some level) foreign suppliers?
- How can DOD trust domestic suppliers (at some level) in the face of potential foreign influence or exposure to insider threat or criminal acts?
- How can DOD trust ICs (at some level) from suppliers who are unable or unwilling to become accredited?
- How can DOD still obtain ICs with specialized performance when commercial suppliers are not interested in the relatively small defense market?

The IC industry continues to consolidate driven by increasing fabrication plant costs, and by 2012, it is expected that number of state-of-the-art fabs will plummet.[15] It is entirely in the realm of possibilities that in the future, there will not be domestic fabs available and the Department will have no choice but to turn to off-shore sources for IC manufacturing. IDA believes that national security interests are best protected by maintaining a strong domestic IC technology and industrial base.

Summary

The information economy is built using semiconductors increasingly supplied by a fast growing, off-shore industrial base. The movement of the domestic industrial base off-shore has generated serious concerns about both security and access to advanced technology, especially for our information-dependent defense systems. Security concerns include both theft of intellectual property related to IC design, a special concern for custom-designed IC, and the potential for tampering with the semiconductors used in our defense systems. The DOD's Trusted Foundry

[15] *IC manufacturing set for restructuring*, EE Times, 11/07/2006.

Program and the complementary Trusted IC Supplier Accreditation were specifically designed and implemented to mitigate these concerns as quickly as possible. The Trusted Foundry Program aggregates defense IC purchases and has generated substantially better access to leading technologies at much lower cost. The Trusted Foundry/Supplier approach should continue to be effective for custom-designed ICs while there remains some domestic fabrication capability, however for broader types of ICs and for other elements of the supply chain, other approaches to addressing the security and access concerns will likely be needed. The Trusted Foundry and Accredited Trusted IC Suppliers have had notable success addressing the security and access issues related to custom-designed ICs.

Mr. Chairman and Members of the Subcommittee, I thank you again for inviting me to participate in this hearing and I would be pleased to answer any questions you might have.