A DARPA Approach to Trusted Microelectronics

Background

To ensure the integrity of critical military systems, Department of Defense Instruction (DoDI) 5200.44 requires that DoD manage risks to the supply and security of certain microelectronic components. Under this Instruction, DoD must provide specific protections—including detecting, avoiding, and mitigating potential threats—based on a component's military importance (criticality).[1] The security environment is fluid, however. Variations in the use and importance of each device, changes in the supplier base, new adversary threats, and the availability of effective threat countermeasures each drive changes in DoD's security needs. Further, no single security solution can provide complete protection for the full range of critical components. That level of protection will take a flexible, technologically-driven, portfolio-based approach to addressing the risks faced.

To evaluate the required protections, the following examination considers DoD microelectronics needs, commercial trends, the microelectronics supply chain, existing threats and vulnerabilities, and ongoing challenges in the current acquisition and security framework. Although this examination primarily covers hardware security during component fabrication and assembly, certain technology solutions could apply across the acquisition process, including in technology development, deployment, and operation.

Demand for military microelectronics

Both the Department of Defense and its foreign military competitors demand access to advanced microelectronics. The Americas comprised more than half of the $3.1 billion market for military and aerospace electronic devices in 2011.[2] Within DoD, these devices support nearly all critical capabilities, among them the global positioning system, radar, command and control, and communications. Demand for defense-related electronics is global, however; foreign governments are bolstering their access to leading-edge microelectronics and leveraging readily available commercial devices for military use.[3] [4]

Although many DoD systems rely on older 90-nanometer (nm) or 130-nm technologies, leading-edge microelectronics offer specific, military-relevant advantages to DoD and its foreign competitors. Today's advanced IC technologies—which generally offer smaller feature (subcomponent) sizes, increased performance, and greater capability—will prove critical to achieving stringent military size, weight, and power (SWaP) requirements. Compared to 90-nm and 130-nm technologies, leading-edge technologies (with feature sizes below 90-nm) could offer a tenfold increase in power efficiency for computational tasks [Figure 1]. These technologies also could enable DoD to increase the range and flexibility of communication and electronic warfare systems and to benefit from developments in big data and machine learning. Several leading-edge ASICs under development at DARPA are intended to deliver revolutionary warfighter capabilities. These ASICs could distinguish and classify radiofrequency signals for 180 hours using a cellphone battery, capture and analyze unprecedented volumes of RF data at high speeds, enable real-time

[1] Department of Defense, "Protection of mission critical functions to achieve trusted systems and networks (TSN)", DODI 5200.44, Aug. 26, 2016. Online: http://www.dtic.mil/whs/directives/corres/pdf/520044p.pdf.
[2] Databeans, "2011 semiconductors in military and aerospace," 2011. Online: http://www.researchandmarkets.com/research/25cb24fa/2011_semiconductor.
[3] Paul Mozur and Jane Perlez, "Concern grows in U.S. over China's drive to make chips," *The New York Times*, Feb. 4, 2016. Online: http://www.nytimes.com/2016/02/05/technology/concern-grows-in-us-over-chinas-drive-to-make-chips.html?_r=0.
[4] Claudette Roulo, "Technology gap closing, top acquisitions official warns," *DoD News*, Nov. 5, 2014. Online: http://www.defense.gov/News-Article-View/Article/603591.

machine learning on small platforms, and allow a single camera to collect varied data across multiple locations.

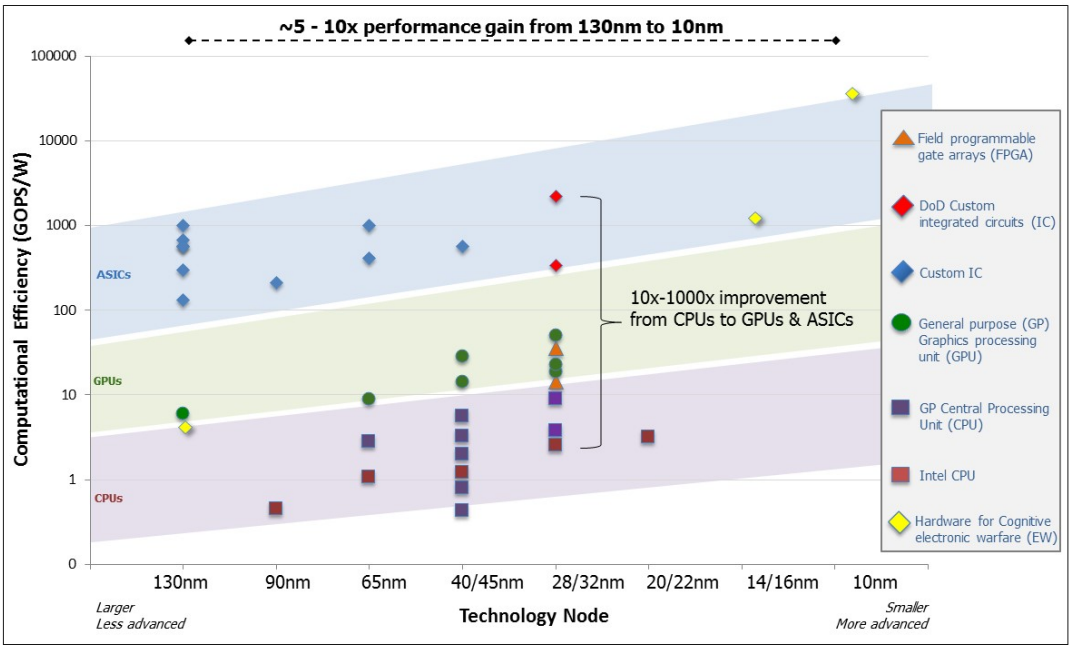

Figure 1. More advanced technologies with smaller feature sizes can offer significant SWaP and performance improvements.[5]

Adopting these newer technologies can help DoD protect against potential threats and maintain an advantage against competitors. Due to the complexity of newer IC technologies, the security threats from reverse engineering, counterfeiting, or cloning are each less pronounced for more advanced microelectronics. Rapid access to leading-edge ICs can also facilitate repeated upgrading of military systems to meet new challenges. As a result, DoD must balance the need for advanced, commercially supported electronics against the security implications of slow-to-update, government-specific IC technologies.

DoD's small market size limits its ability to influence commercial microelectronics firms and imposes unique security and performance requirements that differ from common business practices.[6] Despite its historical importance to the microelectronics sector, DoD today represents less than 1% of sales revenue of the $335 billion commercial global semiconductor industry.[7] Unlike commercial products such as mobile communications and consumer electronics, which drive large production volumes and emphasize yearly upgrades, DoD generally requires low production volumes for devices that could remain in use for decades. DoD often also has unique requirements for radiation tolerance, security, and survivability.[8] As a result, only one leading-edge supplier, IBM Microelectronics, offered to meet DoD's request for a long-term military

[5] Data collected by DARPA from International Solid-State Circuits Conference Papers (2010 – 2013) and other sources.
[6] André Gudger, et al., Written statement before the House of Representatives Committee on Armed Services, Oct. 28, 2015. Online: http://docs.house.gov/meetings/AS/AS06/20151028/104057/HHRG-114-AS06-Wstate-GudgerA-20151028.pdf.
[7] *Ibid.*
[8] Department of Defense Advisory Group on Electron Devices, "Special technology area review on field programmable gate arrays (FPGAs) for military applications, Jul. 2004. Online: http://www.dtic.mil/get-tr-doc/pdf?AD=ADA442913.

microelectronics fabrication contract in the early 2000s.[9] IBM later exited the microelectronics fabrication business entirely. Similar concerns about the availability of fabrication partners exist for non-ASIC electronics alternatives such as field programmable gate arrays (FPGA).

Commercial microelectronics trends

Fabrication at the leading edge increasingly relies on a limited number of highly consolidated, global multinational commercial firms, many of which operate in the United States. In 2015, the semiconductor industry announced or completed more than $100 billion in mergers and acquisitions, including the sale of DoD's most advanced trusted fabrication supplier, IBM Microelectronics.[10] Today, only four companies maintain semiconductor fabrication (foundry) capabilities at 14-nm, the most advanced available feature size: U.S.-based Intel Corporation; Taiwan-based Taiwan Semiconductor Manufacturing Company (TSMC); South Korea-based Samsung; and U.S.-based but Abu Dhabi-owned GlobalFoundries [Figure 2]. Three out of the five 14-nm foundries, however, operate within the United States, including the IBM facilities now owned by GlobalFoundries.

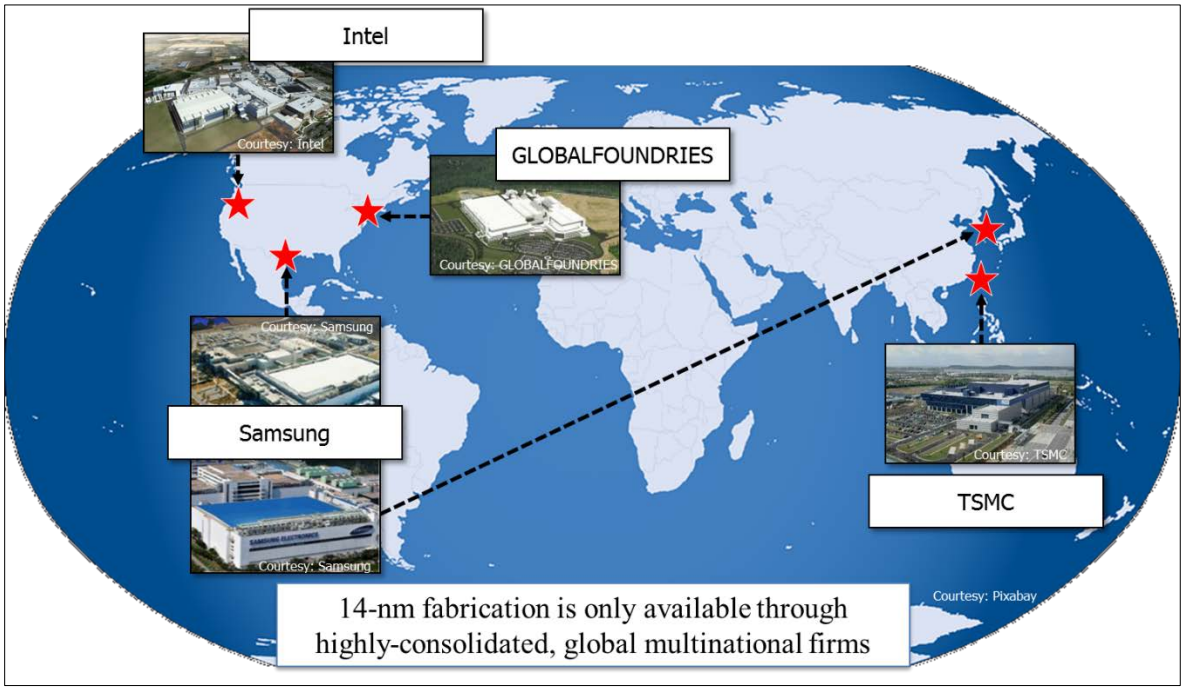

Figure 2. Three of the five leading-edge 14-nm foundries operate within the United States.

High start-up costs, competition for new technologies, and a demand for improved profits will likely drive continued merger activity, further reducing the number of available suppliers.[11] At the leading edge, semiconductor industry competition requires massive investments both in research and development and

[9] Kristen Baldwin, Testimony before the House of Representatives Committee on Armed Services, Oct. 28, 2015. Online: https://www.gpo.gov/fdsys/pkg/CHRG-114hhrg97497/pdf/CHRG-114hhrg97497.pdf.
[10] Dylan McGrath, "IC merger mania hits fever pitch," EETimes.com, Dec. 2, 2015. Online: http://www.eetimes.com/author.asp?section_id=36&doc_id=1328395.
[11] Cromwell Schubarth, "Semiconductor industry expects 2016 to be another big year for M&A," *Silicon Valley Business Journal*, Dec. 9, 2015. Online: http://www.bizjournals.com/sanjose/blog/techflash/2015/12/semiconductor-industry-expects-2016-to-be-another.html.

in foundry construction. Construction costs alone for a new state-of-the-art fabrication plant can exceed $15 billion.[12] Such high start-up costs could not only limit the number of firms providing foundry services but also encourage foundries to prioritize customers that, unlike DoD, demand high manufacturing volumes and drive large revenues. These and other concerns have led DoD to consider methods of bolstering its current trusted supplier policy, which has traditionally relied on domestically-owned and -operated facilities.[13]

Over the next decade, the commercial market will continue to pursue increasingly capable technologies with smaller feature sizes. Semiconductor manufacturers GlobalFoundries, TSMC, Intel Corporation, and Samsung have each announced plans to produce new 10-nm or 7-nm technologies within the next two years and to thereby provide significantly improved device performance and capabilities.[14] In May 2017, Samsung announced a semiconductor roadmap that included technologies from 8nm down to 4nm—enabled by extreme ultraviolet lithography—and fully depleted silicon-on-insulator (FD-SOI) technology at 18-nm.[15] The power efficiency requirements of smartphones and Internet of Things (IoT) applications, which are increasingly driving large yearly demands, are anticipated to foster continued interest in these leading-edge technologies.[16] Insufficient alignment between DoD and the commercial sector, in part due to trust concerns, could make these advances inaccessible to the military.

Advancing beyond 14-nm feature sizes could continue to reshape the microelectronics industry, stressing even the largest firms and emphasizing the need for specialized ICs. New IC generations will likely become available later than predicted under Moore's Law, which had correctly forecast the rapid pace of transistor miniaturization for the past half century.[17] Successive generations could prove even more delayed due to increasing production difficulties and high costs. These challenges may well lead to a declining emphasis on generalized IC solutions—which have exploited the rapid improvements available under Moore's Law—and instead emphasize specialized ICs with more specific performance benefits. DoD policies and acquisition strategies must therefore support engagement with the multinational commercial firms most able to produce specialized ICs near the leading edge. Among the DoD-relevant technologies and capabilities that could be improved by access to such circuits are machine learning, data sorting for recognition of events, and countering electromagnetic threats.

DoD and the microelectronics supply chain

DoD's microelectronics acquisition relies heavily on the commercial sector; acquiring military-customized ASICs, however, can require closer coordination with vendors than would be expected with commercial-off-the-shelf (COTS) products. This coordination, intended to ensure ASIC security and performance, can add new requirements to each phase of the microelectronics acquisition lifecycle [Figure 3]. DoD size, weight, power, and performance requirements, for instance, drive the selection of new and existing circuit intellectual property (IP) blocks during ASIC design. DoD security considerations may also impact the selection of ASIC fabrication and assembly locations, where several hundred unique steps can place more than

[12] Nicolas Mokhoff, "Semi industry fab costs limit industry growth," *EETimes*, Oct. 3, 2012. Online: http://www.eetimes.com/document.asp?doc_id=1264577.
[13] André Gudger, et al., Testimony before the House of Representatives Committee on Armed Services, Oct. 28, 2015. Online: https://www.gpo.gov/fdsys/pkg/CHRG-114hhrg97497/pdf/CHRG-114hhrg97497.pdf.
[14] Mark Lapedus, "10nm versus 7nm," *Semiconductor Engineering*, Apr. 25, 2016. Online: http://semiengineering.com/10nm-versus-7nm/.
[15] Samsung USA, "Samsung set to lead the future of foundry with comprehensive process roadmap down to 4nm", May 24, 2017. Online: https://news.samsung.com/global/samsung-set-to-lead-the-future-of-foundry-with-comprehensive-process-roadmap-down-to-4nm.
[16] Handel Jones, "Whitepaper: semiconductor industry from 2015 to 2025", *Semiconductor Industry Association*, Aug. 4, 2015. Online: http://www.semi.org/en/node/57416.
[17] Tom Simonite, "Intel puts the brakes on Moore's Law," *MIT Technology Review*, Mar. 23, 2016. Online: https://www.technologyreview.com/s/601102/intel-puts-the-brakes-on-moores-law/.

a billion transistors onto silicon chips and combine them into larger devices.[18] During ASIC deployment and integration, unique DoD needs may further necessitate additional steps to customize (or personalize) electronics before they are integrated into military systems. Finally, DoD may pursue additional requirements for the operation, repair, replacement, and disposal of its electronics.

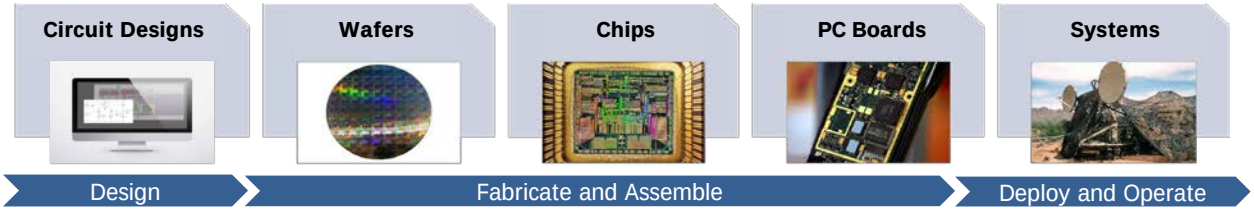

Figure 3. In this simplified microelectronics acquisition lifecycle, components move from design to operation.[19]

To ensure the confidentiality, integrity, and availability of its microelectronics, DoD must consider and contend with several potential risks. Several groups—including the Department of Homeland Security, National Institute of Standards and Technology, Government Accountability Office, and MITRE—have enumerated risks and vulnerabilities to securely acquiring DoD electronics and, more broadly, government information and communications technology (ICT). The respective reports detail threats from both malicious and negligent actors and the vulnerabilities that these actors could attempt to exploit. Within DoD, risks to microelectronics fabrication and assembly have received particular focus. Risks to fabrication and assembly could include the loss of sensitive information, introduction of fraudulent products, insertion of malicious hardware, failures in quality and reliability, and loss of access to electronic components.

Loss of information: Loss-of-information threats involve the unauthorized extraction of sensitive and/or critical program information (CPI) or IP from a design, template (photomask), or manufactured electronic device. Malicious or negligent agents can facilitate CPI loss during fabrication and assembly through the unauthorized production of sensitive hardware or through hardware theft. Known or expected attack types could include:

- Hardware theft: the unauthorized removal of genuine electronic parts (including from a manufacturing or assembly facility), potentially to facilitate IP theft or reverse engineering[20]
- IP theft: the unlawful acquisition of classified, trade secret, or proprietary information associated with microelectronics designs or hardware
- Reverse engineering: actions to determine the underlying structure, function, and composition of a device for the purpose of replicating or defeating the device[21]

Fraudulent products: Fraudulent product threats involve the introduction of counterfeit or unauthorized microelectronics into DoD's supply chain. Fraudulent products include relabeled, recycled, cloned, defective, or out-of-specification devices. Malicious actors could also destroy, damage, or stress hardware (i.e. through

[18] Karen Mercedes Goertzel, "Integrated circuit security threats and hardware assurance countermeasures," *CrossTalk*, Nov. 2013. Online: http://static1.1.sqspcdn.com/static/f/702523/23831194/1383594391887/201311-Goertzel.pdf?token=g1MFzBpKyAdgfTZTDD3wjst4VHY%3D.
[19] In DoD's acquisition lifecycle, this would include material solution analysis, technology maturation and risk reduction, engineering and manufacturing development, production and deployment, and operations and support.
[20] MITRE, "CAPEC-507: Physical Theft" Common Attack Pattern Enumeration and Classification, Dec. 7, 2015. Online: http://capec.mitre.org/data/definitions/507.html.
[21] MITRE, "CAPEC-188: Reverse Engineering" Common Attack Pattern Enumeration and Classification, Dec. 7, 2015. Online: http://capec.mitre.org/data/definitions/188.html.

heating), leading to unexpected and premature hardware failure. Known attack or expected attack vectors could include:

- Counterfeiting: the misrepresentation of an unlawfully reproduced part as being authentic and unmodified, [22] potentially by incorporating components of legitimate but discarded devices
- Cloning: the creation of an exact copy of a genuine part outside of the control of the authorized manufacturer, potentially enabled by IP theft or reverse engineering[23]
- Unauthorized production: the manufacture of microelectronic components by a legitimate supplier without DoD's permission, an act that can threaten the loss of CPI

Malicious insertion: Malicious insertion threats involve the intentional introduction of defects or malicious functions into a photomask or into an individual IC. These defects or functions could permit unauthorized control of a DoD system, unauthorized access to secure logic and data, or mission failure. Malicious insertion threats tend to require advanced knowledge about the targeted system.[24] Known or expected attack vectors could include:

- Design alteration: the modification of a product's specifications, design documents, or physical design to create system weaknesses[25]
- Hardware Trojans: the addition or bypassing of IC logic to enable malicious actions such as disabling encryption or enabling an externally-triggered device failure[26]

Quality and reliability failures: Quality issues, which result from product defects and inadequacies introduced either maliciously or through negligence, can lead to system vulnerabilities or degraded life-cycle performance. Reliability issues, which may not necessarily result from an attack, can yield hardware failures in military-specific environments. Both quality and reliability failures risk compromising unique DoD electronics requirements such as operating lifetime, temperature range, and radiation survivability.

Loss of access: Loss-of-access threats result in DoD having limited or no access to a particular component. Though not specifically a threat to a component's function, loss of access risks DoD's ability to maintain critical systems or to upgrade them in response to new or evolving dangers. Known or expected attack vectors could include:

- Obsolescence: the lack of availability of a particular component, potentially as a supplier ceases producing or supporting the component due to commercial pressures, new versions, etc.[27]
- Supplier loss: the inaccessibility of a particular supplier, potentially due to the supplier's closure or acquisition

[22] "Definitions," Defense Federal Acquisition Regulation Supplement – Subpart 202.1, Oct. 30, 2015. Online: http://www.acq.osd.mil/dpap/dars/dfars/html/current/202_1.htm.
[23] Government Accountability Office, "Counterfeit parts: DoD needs to improve reporting and oversight to reduce supply chain risk," GAO-16-236, Feb. 16, 2016. Online: http://www.gao.gov/assets/680/675227.pdf.
[24] MITRE, "CAPEC-539: ASIC With Malicious Functionality," Common Attack Pattern Enumeration and Classification, Dec. 7, 2015. Online: http://capec.mitre.org/data/definitions/539.html.
[25] MITRE, "CAPEC-447: Design Alteration," Common Attack Pattern Enumeration and Classification, Dec. 7, 2015. Online: http://capec.mitre.org/data/definitions/447.html.
[26] Malek Ben Salem, "Security challenges and requirements for industrial control systems in the semiconductor manufacturing sector," NIST Workshop on Cyber-Security for Cyber-physical Devices, Apr. 23rd, 2012. Online: http://csrc.nist.gov/news_events/cps-workshop/slides/presentation-3_salem.pdf.
[27] "Obsolescence Management," *ACQuipedia*, Defense Acquisition University, Nov. 30, 2015. Online: https://dap.dau.mil/acquipedia/Pages/ArticleDetails.aspx?aid=d3f23881-7a0e-4a3f-83cd-a157e5969666.

- Other supply chain risks: the disruption of a component's production and delivery, potentially due to geopolitical conflicts or natural disasters

To protect DoD capabilities, DoD Instruction (DoDI) 5200.44 requires that DoD apply tailored risk management, based on a system's criticality, throughout the microelectronics acquisition lifecycle. DoDI 5200.44 applies to all information and weapons systems that are determined critical by a DoD acquisition executive or that highly impact the security objectives of confidentiality, integrity, and availability. The Instruction also applies to national security systems, which by definition are integral to weapons systems or to military and intelligence missions and activities.[28] Specifically, DoD requires that risk management techniques help 1) prevent or reduce the likelihood of harmful components entering the supply chain, eliminate vulnerabilities, or make threats more difficult to execute; 2) detect compromised microelectronics; or 3) respond to a compromise by mitigating potential consequences.[29]

For the prevention of threats occurring in the fabrication phase, available or proposed countermeasures include:

- The use of trusted vendors accredited by the Defense Microelectronics Activity (DMEA)
- Domestic, DoD, or Five Eye[30] ownership of suppliers
- Purchasing sensitive equipment via anonymous buys in order to conceal a DoD connection

For the detection of threats occurring in the fabrication phase, available or proposed countermeasures include:

- Visual inspection of ICs to spot counterfeit or stressed hardware
- Validation of ICs and photomasks to a known, trusted design
- Electromagnetic or thermal analysis to spot counterfeit or altered hardware

For the response to threats occurring in the fabrication phase, available or proposed countermeasures include:

- Mandatory reporting of suspected fraudulent products
- Identifying multiple suppliers to allow for switching between component sources
- Maintaining an inventory of spares to combat obsolescence

Globalization and other semiconductor industry trends present a challenge to the traditional DoDI 5200.44 threat prevention model. Under the current security approach, DoD relies on trusted suppliers when acquiring custom ASICs for a DoD end use. This system, which predominantly depends on domestically-owned and -operated facilities, helps to prevent fraudulent product, loss of information, malicious insertion, loss of access, and other risks. As of 2016, however, none of the global multinational firms that manufacture leading-edge 28-nm or 14-nm devices have achieved trusted supplier status for those devices. [31] [32] Moreover, a 2009 DoD report on trusted defense systems concluded that "there is no way to return to a supplier base of 'all-American' companies for the Department's [ICT]." The report also concluded that such an approach was

[28] National Defense Authorization Act for Fiscal Year 1996, Pub. L. 104-106, 116 Stat. 1236, codified at title 40 U.S.C. § section 11103.
[29] DoD Chief Information Officer/Undersecretary of Defense (Acquisition, Technology, and Logistics), "Protection of mission critical functions to achieve trusted systems and networks (TSN)", DoDI 5200.44, Section 4(c), Aug. 25, 2016. Online: http://www.dtic.mil/whs/directives/corres/pdf/520044p.pdf.
[30] DoD's trust approach allows for accreditation of companies from countries within the Five Eye security alliance, namely Australia, Canada, New Zealand, the United Kingdom, and the United States. Only one non-U.S. facility providing foundry services and one non-U.S. facility providing packaging services has been accredited to date.
[31] Defense Acquisition University, "DoD trusted foundry program," Apr. 26, 2016. Online: https://acc.dau.mil/CommunityBrowser.aspx?id=740009.
[32] Defense Microelectronics Activity, "Trusted foundry program: accredited suppliers," Mar. 1, 2016. Online: http://www.dmea.osd.mil/otherdocs/AccreditedSuppliers.pdf.

"neither ideal nor financially feasible on a large scale for a majority of the purposes for which ICT is intended."[33]

One proposed remedy for securing the supply chain, constructing DoD-owned foundries, would likely prove prohibitively expensive. Average construction costs for a leading-edge foundry are expected to reach $15 - $20 billion by 2020.[34] Expected operating costs could also exceed several billion dollars annually, not including significant upgrade expenses.[35] Due to low DoD-demand, a DoD-owned, state-of-the-art foundry would struggle to achieve the volumes required to offset these costs. Further, DoD-owned foundries would not necessarily be immune to security risk.

[33] The Under Secretary of Defense for Acquisition, Technology, and Logistics and Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer, "Report on Trusted Defense Systems In Response To National Defense Authorization Act, Section 254" (Executive Summary and Addendum), Dec. 22, 2009. Online: http://www.acq.osd.mil/se/docs/TrustedSystems-Exec_Summ-wAddendum-wTitlePgNoteinPDF.pdf.
[34] John Villasenor, "Compromised by design? Securing the defense electronics supply chain," Center for Technology Innovation at Brookings, Nov. 2013. Online: http://www.brookings.edu/~/media/research/files/papers/2013/11/4-securing-electronics-supply-chain-against-intentionally-compromised-hardware-villasenor/compromised-by-design-securing-the-defense-electronics-supply-chain.pdf.
[35] Kristen Baldwin and Marie Mak, Testimony before the House of Representatives Committee on Armed Services, Oct. 28, 2015. Online: https://www.gpo.gov/fdsys/pkg/CHRG-114hhrg97497/pdf/CHRG-114hhrg97497.pdf.