United States Government Accountability Office

Testimony
Before the Subcommittee on Oversight and Investigations, Committee on Armed Services, House of Representatives

For Release on Delivery
Expected at 3:30 p.m., EDT
Wednesday, October 28, 2015

# TRUSTED DEFENSE MICROELECTRONICS

# Future Access and Capabilities Are Uncertain

Statement of Marie A. Mak, Director
Acquisition and Sourcing Management

Accessible Version

Chairwoman Hartzler, Ranking Member Speier, and Members of the Subcommittee:

I am pleased to be here today to discuss the Department of Defense's (DOD) efforts to provide access to trusted leading-edge microelectronics.[1] As we reported in April 2015, DOD's ability to provide superior capabilities to the warfighter is dependent, in part, on its ability to incorporate rapidly evolving, leading-edge microelectronic devices into its defense systems, while also balancing national security concerns.[2] However, market trends and globalization of the supply chain have created challenging consequences for DOD. The capital costs associated with production are increasing with each new generation of technology. Leading-edge microelectronics fabrication facilities now require initial capital costs of several billion dollars, in addition to facility operating costs, which can be another several billion dollars annually. Increasing capital costs of manufacturing have led to increased specialization and industry consolidation. Once dominated by domestic sources, microelectronics manufacturing is now largely conducted outside the United States—primarily in Asia—and largely focused on high-volume production driven by demand for consumer electronics. Further, the commercial microelectronics market has short life cycles—commercial firms move on to the latest technology rapidly and have no need to support older technologies. In contrast, DOD requirements for microelectronics are generally low-volume with unique requirements that cover a wide range of technologies, including, in some cases, technologies for which there is no commercial demand. In addition, these requirements are generally needed for long periods because weapon systems are often sustained over decades. As a result, DOD's low-volume requirements have little influence on the commercial market. According to the Defense Science

[1]Microelectronics includes various micro devices, commonly referred to as "integrated circuits," that form the basis of all electronic products. A trusted environment is required to secure national security systems by assessing the integrity of the people and processes used to design, generate, manufacture, and distribute national security critical components, and include fabrication of classified designs. Smaller feature sizes generally represent more advanced technologies and higher performance, with feature sizes of 90 nanometers or smaller generally considered leading-edge.

[2]GAO, *Defense Technologies: Future Access to Leading-Edge Microelectronics is Uncertain*, GAO-15-422RSU (Washington, D.C.; April 15, 2015). This report was issued as "For Official Use Only" given the sensitive and proprietary information involved. Details DOD deemed sensitive and proprietary must be protected from disclosure and are not disclosed in this statement.

Board and DOD officials, the use of foreign suppliers increases opportunities for adversaries to corrupt technologies and introduce malicious code, and for potential loss of national security-related intellectual property.

To mitigate vulnerabilities associated with the increasing reliance on foreign manufacturers for microelectronics and to meet low-volume government needs, DOD and the National Security Agency (NSA) initiated the Trusted Foundry Program for microelectronics in 2004. Implementation of the program included the formation of the NSA's Trusted Access Program Office, which managed a sole-source contract with the IBM Corporation—the only U.S.-based company able to meet DOD and intelligence community needs for trusted leading-edge microelectronics—to provide government-wide access to these types of microelectronics. In 2006, the Trusted Foundry Program was expanded to include firms offering mature technologies and became the "trusted supplier program." Further, the Duncan Hunter National Defense Authorization Act for Fiscal Year 2009 required DOD to develop a strategy to ensure access to trusted sources of microelectronics.[3] In response, DOD developed its Trusted Defense Systems Strategy, which includes its trusted supplier program for providing access to critical microelectronics.

I am here today to discuss the extent that the trusted supplier program provides for DOD's current and future access to trusted microelectronics. This testimony largely leverages our April 2015 sensitive but unclassified report on DOD access to leading-edge trusted microelectronics. This statement also includes updates to information on the transfer of IBM's microelectronics business based on program documentation and discussions with industry and DOD officials that we conducted in September and October 2015. In addition, the statement draws on some conclusions from our October 2008 work on the defense supplier base,

[3]Pub. L. No. 110-417, § 254 (2008).

confirmed by DOD officials in 2015, and the Defense Science Board Task Force on High Performance Microchip Supply.[4]

For our April 2015 report, we reviewed DOD's trusted supplier program and policy guidance documents.[5] We also analyzed utilization data for trusted suppliers and interviewed three of the top defense contractors based on trusted supplier utilization data. In addition, we interviewed officials in the offices of the Secretary of Defense, Defense Microelectronics Activity, NSA, Defense Advanced Research Projects Agency, Intelligence Advanced Research Projects Activity, and Institute for Defense Analysis. For further details on the scope and methodology, see our April 2015 report. We conducted the work on which this statement is based in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

## DOD's Future Access to and Capabilities from Trusted Leading-edge Microelectronics is Uncertain

A decade ago, the Defense Science Board Task Force on High Performance Microchip Supply concluded that DOD had "no overall vision of its future microelectronics components needs and how to deal with them. Technology and supply problems are addressed as they arise. An overall vision would enable the Department to develop approaches to meeting its needs before each individual supply source becomes an emergency."[6] In addition, the report called for the U.S. government, DOD, and its suppliers to establish a series of activities to ensure that the

[4]GAO, *Department of Defense: A Departmentwide Framework to Identify and Report Gaps in the Defense Supplier Base Is Needed*, GAO-09-5 (Washington, D.C.; October 7, 2008). The Defense Science Board, established in accordance with the provisions of the Federal Advisory Committee Act (FACA) of 1972 (5 U.S.C., Appendix, as amended) and 41 C.F.R. 102-3.50(d), provides independent advice and recommendations on matters relating to the DOD scientific and technical enterprise.

[5]GAO issued this report based on a House Armed Services Committee provision in a bill for the Howard P. "Buck" McKeon National Defense Authorization Act (NDAA) for Fiscal Year 2015. H.R. Rep. No. 113-446, at 179 (2014).

[6]Department of Defense, Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, *Report of the Defense Science Board Task Force on High Performance Microchip Supply* (February 2005).

United States maintains reliable access to the full spectrum of microelectronics components. Moreover, it acknowledged that the pace of technology development shifting to offshore locations was alarming because of the strategic significance this technology has on the U.S. economy and the ability of the U.S. to maintain a technological advantage in DOD, government, commercial, and industrial sectors. At that time of its review, the Defense Science Board strongly recommended urgent action to be taken.

In April 2015, we found, as part of DOD's Trusted Defense Systems Strategy, the trusted supplier program was, and still is, a primary risk reduction technique for acquiring certain microelectronics for use in mission-critical components in DOD systems. In 2006, DOD began expanding the number of trusted suppliers to establish a trusted supply chain for mature "non-leading-edge" technologies. At that time, the Defense Microelectronics Activity, under the Office of the Secretary of Defense and in conjunction with other organizations, finalized criteria for trusted microelectronics suppliers deemed as "trusted" through an accreditation process, which included obtaining facility and personnel security clearances. As of August 2014, there were 63 other trusted suppliers in addition to IBM, including 15 with fabrication capabilities. Although these other suppliers do not have the leading-edge capabilities of IBM, they do provide access to a range of mature technologies. However, industry officials stated that use of accredited suppliers other than IBM has been minimal primarily because they do not have the same technologies available, especially at the leading edge. Despite DOD's efforts to expand the number of trusted suppliers, the Department's strategy did not address alternatives for leading-edge microelectronics. DOD's strategy focused on two critical elements of risk: integrity—keeping malicious content out, and confidentiality—keeping critical information from getting out. However, it did not address the risk of relying on a single source. For access to leading-edge trusted microelectronics, DOD's strategy since 2004 has been to rely on IBM as their sole-source provider of leading-edge trusted microelectronics.

In October 2014, IBM announced that its microelectronics fabrication business may be acquired by GlobalFoundries—a U.S.-based foreign-owned entity, subject to completion of applicable regulatory reviews. After this announcement, DOD initiated several actions to identify the risk of potential loss of access to leading-edge microelectronics and to identify and assess alternatives. By July 2015, GlobalFoundries announced that it cleared U.S. regulatory review and it completed the acquisition of IBM's microelectronics business. As a result, continued future access to the

technologies formerly provided by IBM is uncertain. Our work in April 2015 reviewed potential near-term options for access to IBM foundry services, including accredited trusted suppliers other than IBM, other U.S.-owned leading-edge on-shore foundries, and offshore foundries. Although the details of this work are sensitive, based on limitations DOD and defense industry officials described to us, there are no near-term alternatives to the foundry services formerly provided by IBM. We also reviewed potential longer-term options for access, including ongoing research into verification techniques and alternative manufacturing approaches, and a possible government-owned fabrication facility, the details of which are sensitive. However, we did note that these longer-term options all have associated risks and limitations.

As far back as our October 2008 report, and confirmed by DOD officials in 2015, we found that increasing globalization in the defense industry has intensified debate over the use of foreign versus domestic suppliers and presents uncertainty over the ability of the United States to maintain military superiority in critical technology areas. Moreover, as the defense supplier base has consolidated into a few prime contractors, competition has been reduced and single source suppliers have become more common for components and subsystems. This is definitely the case for defense microelectronics. By not addressing alternative options when the Defense Science Board first raised them as urgent issues and by relying on a sole source supplier for leading-edge microelectronics, DOD now faces some difficult decisions with potentially significant cost and schedule impacts to programs that rely on these technologies, as well as national security implications.

Chairwoman Hartzler, Ranking Member Speier, and Members of the Subcommittee, this completes my prepared statement. I would be pleased to respond to any questions that you may have at this time.

## GAO Contact and Staff Acknowledgments

If you or your staff has any questions about this statement, please contact Marie A. Mak at (202) 512-4841 or MakM@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. GAO staff who made key contributions to this testimony are Lisa Gardner, Assistant Director; Bradley Terry; Mary C. Diop; Stephanie Gustafson; Andrew Redd; Penney Harwell Caramia; Joseph Kirschbaum; Timothy Persons; and Sylvia Schatz.