A DARPA Approach to Trusted Microelectronics

Executive Summary

Microelectronics support nearly all Department of Defense (DoD) activities, enabling capabilities such as the global positioning system, radar, command and control, and communications. Ensuring secure access to leading-edge microelectronics, however, is a challenge. Rapid progress in the global semiconductor industry and the sophistication of U.S. adversaries who might target the military supply chain suggest the need for an updated microelectronics security framework.

The Defense Advanced Research Projects Agency (DARPA) is developing a portfolio of microelectronics protections. These countermeasures could enable a technology-driven approach to component protection, increase security, and broaden access to the most advanced microelectronics products. DARPA programs aim to verify the origin and function of sensitive devices, to obscure the purpose of these devices, to protect intellectual property (IP), and to expand DoD’s supplier base. The resulting technologies are anticipated to help ensure the provenance, security, and reliability of the electronic components most likely to drive military capabilities over the next decade.

Under current DoD policy, acquiring custom, application-specific integrated circuits (ASICs)—components that DoD can tailor to its unique military needs—requires the use of government-accredited “trusted suppliers.” This policy-based protection approach aims to provide an assured chain of custody for integrated circuits (ICs), avoid supply disruptions, prevent tampering, protect against unauthorized reverse engineering, and avert the theft of critical program information (CPI).

Current policy, however, can limit DoD’s ability to fully leverage the domestic and global microelectronics supplier base. The Department of Defense is therefore evaluating an alternative microelectronics security framework that emphasizes both flexible access to the commercial sector and high levels of security. This approach would provide an additional pathway for securing custom microelectronics, particularly for those advanced military capabilities with low size, weight, and power (SWaP) demands. It would also emphasize the acquisition of leading-edge commercial capabilities and rapid technology modernization, which is helpful for avoiding and responding to new threats. DARPA and other government agencies are working to enable this framework by developing technology-driven microelectronics protections that DoD can selectively apply based on need. The potential security measures are described below, grouped into multiple classes based on the expected deviation from commercial supplier best practices.

- **Verification and validation countermeasures** would protect against faulty or maliciously altered microelectronics by applying commercial best practices and using DARPA-developed imaging techniques to verify that components function as specified.

- **Obscuration and marking countermeasures** would circumvent IP exploitation, hardware theft, and counterfeiting by either concealing the IP expressed in an electronic component or enabling device authentication.

- **Functional disaggregation countermeasures** would increase protection against IP exploitation and maliciously altered parts and permit rapid ASIC upgrades and redesigns by separating microelectronics into functional, independently manufactured components.

- **Fine disaggregation countermeasures** would protect against maliciously altered components and IP exploitation by further separating sensitive microelectronics into non-functional components, an increasing deviation from standard commercial processes.
- **Transience countermeasures** would protect the IP in DoD microelectronics by enabling the on-command destruction of lost, misplaced, or end-of-life ASICs

- **Government-proprietary solutions**, which include classified techniques, would enable DoD to approach advanced multinational semiconductor corporations while maintaining high levels of trust

In response to a quickly changing semiconductor industry and sophisticated adversary capabilities, the above countermeasures could help DoD better ensure the security of its microelectronics. Moreover, the technologies under development have the potential to deliver security while enabling improved DoD collaboration with the many R&D-intensive commercial suppliers that drive the global microelectronics market. That increasing collaboration could alleviate the tension between relying on government-controlled ICs, which offer security but tend to update slowly, and leveraging leading-edge commercial ICs, which improve rapidly.

Although this examination of the issue focuses primarily on maintaining or enhancing the protections currently available during ASIC manufacture, several of the identified countermeasures could improve security across the acquisition lifecycle. For instance, verification and validation countermeasures could apply to ASIC design; obscuration and marking to post-manufacture deployment; and fine disaggregation and transience to end-of-life-disposal. Moreover, the required countermeasure classes could evolve to protect non-ASIC microelectronic components. Starting in fiscal year (FY) 2017, various pilot projects and demonstration programs could provide the confidence required to fully pursue this microelectronics security approach and its expansion.