NDIA

Trusted Microelectronics

Joint Working Group

Team 3 Summary

Trustable Microelectronics Standard Products

July 2017

DISCLAIMER: The ideas and findings in this report should not be construed to be official positions of any of the organizations listed as contributing members of this Joint Working Group or the membership of NDIA. It is published in the interest of information exchange between Government and Industry, pursuant to the mission of NDIA.

Team 3 - Trustable Microelectronics Standard Products

Catalog microelectronics components and technologies designed and produced for commercial markets are often used in defense systems and can be critical to the system's function and operation. While the Department of Defense (DoD) has established trust criteria for sourcing custom integrated circuits used in covered systems, there is not an equivalent trust criteria covering commercial standard parts. Team 3 of looked at this question by analyzing adjacent non-defense industries and the lifecycle of standard products. Several adjacent industries have concerns similar to DoD's and thus present an opportunity to join their initiatives to create new standards and controls.

While commercial catalog components come without any evidence of meeting any defense specific trust or assurance requirements, visibility into commercial practices can provide for some level of characterization of trust and assurance. It should be noted that Defense Microelectronics Activity (DMEA) recently created a process to allow commercial parts to achieve a Category II level of Trust. This new criterion requires participation by the vendor and as such is not addressed in this paper.

Summary of Findings and Recommendations

There are tremendous upsides with using commercial microelectronics. For example, defense systems can be afforded highly advanced components such as FPGAs, memory chips or receiver chips that might have cost over $100 million to develop and bring to market, but sell for a small fraction of the development cost from amortizing that cost across the commercial applications' volume manufacturing. Catalog chips that are in wide use would conceivably be subject to global security challenges and evaluations with corporate documentation of errata or issues of fixes addressed via firmware updates etc., thus improving the component's reliability over time.

On the downside, using commercial components coupled with long-lived defense systems can create long-term obsolescence problems for Defense systems as the life-cycle of chip technologies becomes shorter and shorter. From a security perspective, a commercial component might be susceptible to an unpublicized vulnerability for an adversary to exploit if enough effort were spent examining the chip. Of course, it is possible for a custom or semi-custom chip to have an analogous flaw, but if it were produced using a trusted flow it is presumed to be difficult for an adversary to obtain the chip and the design information needed to exploit the flaw.

The NDIA Trusted Microelectronics Joint Working Group Team 3 recommends that DoD:

- *Develop and employ a consensus approach for establishing categories of trustworthiness for catalog chips based on risks, commercial practices, use of standards (SAE, ISO or Open Group accreditation procedures etc.) or quantifiable supplementary information that can be supplied with respect to a catalog chip. This approach should lead directly to a methodology for assessing individual microelectronics used in critical roles in defense* *systems. Using a categorization approach to establish various levels and mitigations will require expert inputs and debates but will provide the best long-term solution for DoD.*

- *Partner with non-defense industries working with commercial microelectronics companies to enhance security status and affordability of catalog chips in areas like industrial standards and supply chain practice.*
- *With vendor participation, the DMEA Category II criteria could be used for an additional level of trust above the basic best commercial practice.*

--END--