Trusted Microelectronics

Joint Working Group

Team 3 White Paper:

Trustable Microelectronics

Standard Products

July 2017

(This Page Intentionally Blank)

I. FOREWORD

Over the course of the past 70 years, the United States Government (USG) microelectronics needs for national security applications [Department of Defense (DoD), Department of Energy National Nuclear Security Administration (DOE-NNSA), and the Intelligence Community (IC)] and the semiconductor industry have been intertwined. Indeed, the U.S. semiconductor industry in part grew out of USG funded Research and Development (R&D). In recent decades, however, commercial applications and high-volume production have dwarfed USG demand, such that USG purchases (be it direct or through a third party) now account for a very small part of total production, resulting in commercial market forces driving the industry. As noted by the most recent President's Council of Advisors on Science and Technology (PCAST) report,

> "The global semiconductor market has never been a completely free market: it is founded on science that historically has been driven, in substantial part, by government and academia; segments of it are restricted in various ways as a result of national-security and defense imperatives; and it is frequently the focus of national industrial policies. Market forces play a central and critical role. But any presumption by U.S. policymakers that existing market forces alone will yield optimal outcomes – particularly when faced with substantial industrial policies from other countries – is unwarranted."[1]

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. But, while commercial markets provide powerful incentives for innovation, quality, and cost/bit/function these products and their supply chains do not provide DoD with insight to the trustworthiness of the electronic components and can introduce unknown risk into a defense system.

Team 3 of the NDIA Trusted Microelectronics Joint Working Group (TM JWG) looked at methods to evaluate the trustworthiness of commercial components 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.

[1] https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_ensuring_long-term_us_leadership_in_semiconductors.pdf, "PCAST Ensuring Long-Term U.S. Leadership in Semiconductors"

II. PAPER DISPOSITION

This paper is formally submitted to the Assistant Secretary of Defense for Research and Engineering, Office of the Undersecretary of Defense for Acquisition, Technology and Logistics. Permission is granted to widely distribute and quote with proper attribution. The paper will be made available on the National Defense Industrial Association website (http://www.ndia.org/divisions/working-groups/tmejwg as a reference resource.

III. PRINCIPAL CONTRIBUTORS

The team was composed of 28 dedicated team members from 20 organizations who all contributed diligently to this work.[2]

The Trusted Microelectronics Joint Working Group Team 3 consisted of the following members:

Bryan Brady	Avnet
Dean Brenner	Honeywell International
Dan Campion **	Honeywell International (former)
Edward Chatters	Contract Support to ODASD(SE)
Saverio Fazzari	Booz Allen Hamilton
John Hallman	MacAulay-Brown, Inc.
Kenneth Heffner	Honeywell International
Mike Holmes	Sandia National Labs
Kenneth Lebo*	Jacobs
Neal Levine	Defense Microelectronics Activity
Dave Meshel	The Aerospace Corporation
Greg Orne	Honeywell International
Daniel Radack	Institute for Defense Analyses
Vashisht Sharma	Institute for Defense Analyses
Christopher Sims	Naval Surface Warfare Center Crane
Roger Van Art	Jazz Semiconductor Trusted Foundry
David Weaver	SRI International

*Team Leader
** Founding team leader

[2] Disclaimer: This white paper is a product of the group at large and does not necessarily reflect the beliefs or endorsements of listed individuals or their employers.

IV. SOURCES

Team 3 reviewed materials from recent supply chain issues and analysis. Some team members were also participants in separate efforts to consider FPGA concerns and identified relevant overlaps especially in the areas of adjacent industries and potential partnering leverage.

Team 3 surveyed industry experts on business practices, procedures, and industrial standards that can mitigate known and unknown risks in microelectronics design, fabrication and packaging for commercial applications. We sought to identify the measures that companies had in place to protect their products, including those that are unique to specific operations - such as the controls they describe to their customers to assure them of their product's integrity. Results were used to develop our recommendations, particularly those to improve acquisition of commercial integrated circuits for defense systems.

Detailed survey responses were received from Analog Devices, Cypress Semiconductor, GLOBALFOUNDRIES, Honeywell International, Intel Programmable Solutions Group, Jazz Semiconductor Trusted Foundry, Micron, Microsemi Corp, ON Semiconductor, Qorvo, SRI International and Xilinx. The written survey was augmented with phone interviews in many cases.

V. TABLE OF CONTENTS

(This Page Intentionally Blank)

1 EXECUTIVE SUMMARY

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 to Trust criteria covering these commercial standard parts. What, if anything, can be said about the trustworthiness of standard parts? Team 3 of the NDIA Trusted Microelectronics Joint Working Group (TM JWG) 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.

TM JWG Team 3 offers two main recommendations for consideration: First, DoD should establish criteria for assigning a level of assurance to standard products in keeping with their intended use in the system. An assessment-based approach that considers risks, vulnerabilities and threats to inform programs would parallel DoD's methodology with other areas of concern. Second, Team 3 sees opportunity to leverage growing concerns in adjacent non-defense industries with integrity issues of the underlying microelectronics components. Engaging with these industries' risk mitigation process could ensure that new standards or controls align with DoD's main concerns.

2 INTRODUCTION and BACKGROUND

Standard products, as the term is used in this paper, are commercial catalog microelectronics components and technologies designed and produced for commercial markets, but used in defense systems. Typically, defense systems contain commercial catalog microelectronics and technologies (often referred to as commercial off-the-shelf or COTS), military/aerospace catalog microelectronics along with custom/semi-custom components. The NDIA Trusted Microelectronics Joint Working Group Teams 2 and 4 studied important aspects of the latter with respect to security and trustworthiness and assurance for defense use, while Team 1 looked at the system pull for microelectronics to extrapolate future microelectronics needs. This report describes Team 3's work to assess the trustworthiness of purely commercial microelectronics sourced from the merchant commercial industrial base but acquired for defense use. Given the wide variety of commercial

components and the attractiveness of their use, it is a practical reality that DoD will want to make use of commercial microelectronics wherever it makes sense and is appropriate.

2.1 Statement of Problem

Commercial microelectronics such as microprocessors, digital signal processors, signal conversion, field programmable gate arrays, software-defined radio receivers, and memory, etc., may play critical roles in defense systems components. In fact, many of the military/aerospace catalog microelectronics are versions of commercial components that have been packaged in compliant materials and typically tested and validated for use in military environments such as extended temperature operation, radiation tolerance or other military/aerospace requirements (e.g., hermeticity).

Thus, most microelectronics used in defense applications are either directly commercial components, or are nearly entirely commercial and may only differ in the last steps of packaging and test. Of course, there can be components for military applications that are specially designed, manufactured, and packaged. Some radiation hardened microelectronics may fit this category, but many components in defense systems are essentially commercial components or derived directly from commercial versions. Further complicating matters, defense systems may be comprised in whole or part by hybrid sub-systems in which commercial electronics assemblies with multiple components are integrated with other military grade hardware, including custom or specialized hardware not generally in the commercial domain.

Given the importance of commercial microelectronics in defense systems, Team 3 focused on the questions of whether, and how, typical commercial components could be used in defense applications that have needs for trusted microelectronics, and if security concerns could be managed when using commercial chips. For example, are there best (or at least better) practices used by merchant commercial microelectronics suppliers to assess qualities such as trust and assuredness?[3]

Team 3 focused on answering these questions in the context of purely commercial microelectronics that are available in the marketplace, not on alternatives to "Trust" or "assurance" models. The team looked for practices or technologies already in place and not for research opportunities as that was in another team's domain.

2.2 Why Is This Topic Important?

The microelectronics hardware in a system is critical to the system's performance and it must function properly to preserve confidence in the system itself. Hardware provides the electrical functionality – the signal conditioning and processing, the memory, the communications, the data

[3] In this document, "trust" refers to a level of confidence that there are protections against an adversary acting maliciously in the supply chain creating vulnerabilities that might lead to system or mission security consequences. "Assurance" is a level of confidence that a component is free of vulnerabilities (both intentional and unintentional) which might lead to system or mission security consequences.

processing, control signals, the actuation in many cases. Even when electrical systems and circuits are built with redundancy and fault tolerance in mind, each component is critical to the complete system's function, and everything from the power supply components to the signal chain chips are important from functional and operational perspectives. Furthermore, encryption keys, roots of trust, algorithms, and other sensitive information that are designed into the hardware must be protected. Even electrical components seemingly ancillary to critical functions can provide entry points for adversaries. And once fielded, it is very difficult and expensive to address problems with hardware.

DoD has both generalized and specific security concerns regarding its systems, including the trustworthiness of the components that comprise a system and those components' supply chains. Concerns over software vulnerabilities and cybersecurity are not especially new,[4] but there is a growing concern about the underlying hardware, including the chips and their points of origin, that are being installed into defense systems.[5] The DoD typically has little insight into the details of design information, intellectual property (IP) containment, and the components' manufacturing, making it difficult to appraise parameters like trustworthiness. While the practical reality is that DoD (including DoD programs, primes, subs, suppliers, etc.) will continue to procure commercial components for use in systems, there will also continue to be security concerns beyond those typical of commercial entities. Some of the concerns over component trustworthiness arise from long system lifecycles and hazardous use conditions and degree of confidence required in times of need.

DoD defined and implemented an accreditation process for Trusted suppliers of certain microelectronics technologies and supply chain components, [6] but there are not presently any forces that are driving a commercial equivalent of Trust for standard products. Most companies in the commercial semiconductor products business follow standards and procedures generally accepted as sufficient for commercial purposes, but DoD's unique concerns led to the establishment of Trust criteria. As previously mentioned there is a recently created DMEA process that allows 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.

There is also the issue of security of the individual component, as well as with the higher-level assembly. The system consists of subsystems that interact with active and passive components internal to these subsystems and sub-assemblies, with the electronic hardware typically executing some form of software code.

[4] John Villasenor, "Compromised By Design? Securing the Defense Electronics Supply Chain" (https://www.brookings.edu/wp-content/uploads/2016/06/Villasenor_HW_Security_Nov7.pdf)
[5] P.W. Singer, "Hacked Hardware Could Cause The Next Big Security Breach" (http://www.popsci.com/nowhere-to-hide)
[6] See the Defense Microelectronics Activity website: Trusted Supplier Accreditation Program, http://www.dmea.osd.mil/trustedic.html (2017)

Mapping security from the system level to the component level is more art than accepted science. At the component level, there is typically a complex array of interacting circuits, often with IP procured from a variety of sources, which further complicates the challenge of ensuring trust and assurance. Again, at the component level, some microelectronics are highly complex with billions of transistors interconnected and some have just a few transistors. Some microelectronics are designed to be general purpose but get personalized via software control and programming by users, and some are hardwired; some have characteristics of both. Concerns may therefore vary, but generally the greater complexity and/or programmability in a component, the greater the potential for security concerns.

The long-term overall interest in the security of field programmable gate arrays (FPGAs) stands out as an example: a state-of-the-art FPGA consists of billions of transistors that are user programmable, as well as a host of other on-chip resources that have varying degrees of user accessibility. Further, nearly all FPGAs, including some that meet military specifications, are based on commercial components and most are volume manufactured before being put into wide commercial use, suggesting that security concerns would be discovered through broad deployment. Nevertheless, there are myriad difficulties in translating system-level concerns with security down to the component level as interconnections between components make this undertaking more an art than engineering analysis.

DoD has defined processes to identify critical program information (CPI) and critical components (CC) and has provided guidance to programs for protecting CPI and CC including certain types of custom chips (see DoDI 5200.44). DoD guidance specifies that covered custom and application–specific hardware deemed to be CPI must be procured from Trusted sources, but DoD cannot impose special processes on commercially produced microelectronics at the component-level without losing most of the benefits, including volume production methodologies, reliability, and cost.

Nevertheless, protecting microelectronics and its supply chain, along with processes to evaluate the component's integrity, are important to reduce an adversary's opportunity to undermine a mission through an undetected defect contained in the system's electronic hardware.[7] The focus has been placed on the microelectronics because they now can contain extremely complex programmable circuits that can profoundly affect system functionality and operation in ways that are difficult to overcome if the components themselves have been subverted or contain defects that open channels that an adversary can use to their advantage.[8] Adding just a few logic gates to a chip that has millions or billions of transistors, or discovering undocumented chip states and modes, can be sufficient for adversaries to impact mission success. To advance their aims, adversaries could obtain

[7] T.S. Perry, "Why Hardware Engineers Have to Think Like Cybercriminals, and Why Engineers Are Easy to Fool," IEEE Spectrum, May 2017. (http://spectrum.ieee.org/view-from-the-valley/computing/embedded-systems/why-hardware-engineers-have-to-think-like-cybercriminals-and-why-engineers-are-easy-to-fool)
[8] Ted Marina and Jenny Yao, "Hardware Security in the IoT" (http://embedded-computing.com/articles/hardware-security-in-the-iot/)

design information or use insiders to exploit unintentional insecurity in the system's microelectronics.

DoD is not alone in these concerns about microelectronics integrity. Given the state of concerns in other products and systems, Team 3 determined that DoD may be able to leverage adjacent industries' interests in the assuredness of the underlying microelectronics technologies to forge alliances and standards where appropriate. Team 3 acknowledges the difficulties in attaining integrated alignment given the disaggregated nature of DoD's program execution and suggests a central coordinating office serve as a focal point.

3 METHODOLOGY

The Trusted Microelectronics Joint Working Group Team 3 considered adjacent industries, particularly automotive and IoT, as the best aligned for collaboration and sharing of practices. We examined prior efforts to collect best practices and codify them in NIST and other standards. DoD has been developing a framework intended as a tool to aid acquisition decisions along these lines. Finally, we interviewed experts from the commercial semiconductor industry and sent a questionnaire to a broad set of commercial semiconductor companies seeking to better understand their controls, practices and procedures with their product flows, and to identify salient methods they may have implemented to protect their products' security.

4 RESULTS

Team 3 found that the DoD is not alone in its microelectronics security concerns; several non-defense industries have similar concerns over their component supply chains and suppliers.

Banks and financial institutions, retail, infrastructure, industrial industries, etc. are concerned about trust, and assuredness in their transactions, services and products. In the consumables industries, food suppliers and pharmaceutical companies have concerns over supply chains and safety/health issues with federal agencies devoted to providing regulation and oversight. Additionally, some manufacturers of luxury goods and retailers have been concerned about counterfeiting for decades and are motivated to prevent damage to their brand. The concerns over counterfeit goods and parts extend into nearly all categories of durable goods.

There are increasing concerns about the security of hardware and software being used in the Internet of things (IoT) and by automotive companies in current cars for driver assistance and

telematics, as well for next generation connected cars and future autonomous vehicles.[9] ***Team 3 acknowledges that some of these security concerns are not new and have not been adequately addressed in the past due to business decisions and failures of market support for more secure chips if those chips also are more expensive than less secure counterparts.***

Given the state of concerns in other areas, Team 3 assessed that DoD ought to be able to better leverage adjacent industries' interests in the assuredness of the underlying microelectronics technologies and join with groups to forge alliances and standards where appropriate. ***Team 3 acknowledges the difficulties in attaining integrated alignment given the disaggregated nature of DoD's program execution and suggests a joint coordinating office might serve as a focal point for ensuring that DoD's programs that need secure microelectronics have an identifiable resource with domain expertise.*** That office could also serve to coordinate among programs to ensure cost-effective approach for baseline technologies and components, and provide leverage in the commercial domain such that initiatives addressing security of microelectronics provide DoD with sustainable outcomes.

NIST and others (SAE, ISO, etc.) have published standards that touch on this area. The Trusted Microelectronics Joint Working Group Team 3 reviewed the DoD-sponsored work to aggregate relevant security standards/controls for electronics components, entitled "Trustworthy Supplier Framework.[10] (TSF)" This framework, developed by a DoD support team, uses NIST SP 800-161 as a foundational organization of supply chain vulnerabilities and mitigation practices. Designed to be useful when purchasing electronic components outside the traditional defense base, the targeted users are acquisition and program managers.

The TSF provides a tool to assists DoD buyers select appropriate supply chain risk mitigations when buying standard products, identifying actions a buyer can take to increase confidence in a supplier's trustworthiness. The TSF essentially organizes and compares the landscape of existing supply chain standards and industrial practices so a buyer can better understand the risks associated with a specific supplier and make cost-effective decisions that meet program risk requirements within budget. Team 3 determined that the TSF is a step in the right direction for acquisition agents but is more useful for covering broader supply chain risks. While some of the categories of controls are applicable to best supply chain risk concerns at the component level, most of the microelectronics being used in defense systems are from commercial markets. As such the application of the TSF against the best practices used by commercial companies offers an alternative to requiring suppliers to implement defense unique practices. There is an ecosystem of commercial semiconductor companies that supply components to defense systems; each has its own supply chain practices and this approach might give DoD some degree of confidence for concerns beyond those covered by the standard commercial warranty.

[9] Ted Marina and Jenny Yao, "Hardware Security in the IoT" (http://embedded-computing.com/articles/hardware-security-in-the-iot/)
[10] Trustworthy Supplier Framework, 2015 NDIA Systems Engineering Conference (http://www.dtic.mil/ndia/2015/system/17976_Cohen.pdf)

Commercial companies provided responses to Team 3's inquiry on individual company's product integrity practices. Responses were received from a good cross section (see SOURCES section) of the semiconductor industry and detailed the procedures and methods used to ensure the products sold to customers conforms to the stated specifications. A consensus response emerged that commercial companies were most sensitive toward – that being one of their reputation and brand. If defects are found in the product, it can reflect poorly upon the manufacturer and can harm their business. Many companies have internal workflows and processes for both new products and existing products, some of which were described in detail to the team. These management approaches, including the reporting chains, lend credence to companies' dedication to quality, reliability, and specification conformance and demonstrate a serious commitment to identifying and correcting errors as part of the new product and fielded product support.

Most companies have mechanisms for addressing defects discovered by the end user, some of which include fairly elaborate procedures for the handling of, and responding to, latent defects. Without exception, the companies were concerned about their reputation and brand in the commercial space and several remarked that this alone was a powerful incentive to design and manufacture and support products that have integrity and conform to their specifications. Of particular interest to Team 3 were responses from major merchant FPGA suppliers who provided Team 3 members with details of their internal processes for assuring the integrity of their programmable products along with their own perspectives of which factors were of greater importance and how their mitigations provided superior coverage of concerns. While Team 3 received some remarkably detailed responses about how products are developed and manufactured, there were clearly no commercial equivalents or analogs to the "Trust" accreditation.

From this information, Team 3's assessment is that commercial markets provide powerful incentives for innovation, quality, and cost/bit/function but this alone does not necessarily provide DoD with insight to the trustworthiness of any specific component. Qualities like assuredness or security have no directly measurable quantities; therefore, Team 3 determined that the DoD needs to undertake efforts to understand the security status of commercial products and their sources to characterize the risks of using critical applications.

Unfortunately, no single answer was found to the original question posed about the security implications of using commercial chips. Rather, it is conceivable that an approach for assessing the security of individual chips could be developed through a consensus process that establishes categories of security (or assuredness or trustworthiness, etc.) based on evaluation of risks and has a basis in commercial practices or reasonable requests by DoD for information from catalog chip manufacturers. ***A consensus approach that embodies industry inputs is more likely to result in enhancing the understanding of security status of individual catalog chips and preserving a competitive market among suppliers, giving defense programs as many options as possible for cost, schedule, and performance considerations.*** This approach can lead to a methodology for evaluating individual chips and suppliers based on their product integrity and supply chain practices and should

be designed to enable the DoD to leverage commercial practices to the greatest extent possible to maintain the advantages of using catalog chips while avoiding imposing unworkable burdens on commercial companies.

5 RISKS OF INACTION

Ignoring risks in commercial components can leave systems susceptible to malicious threats of increasing potential consequence and severity. Therefore, DoD needs to better understand the assuredness of the underlying microelectronics components in its systems to understand how best to protect the system across its lifecycle. To address this risk, the DoD should undertake an effort to understand and quantify security risks associated with specific components perhaps developing a prioritized list. An adversary who can undermine core hardware may make our systems vulnerable, inoperable, or worse in ways that can't be overcome without enormous cost and efforts based on program needs and potential consequences, then utilize experts to develop guidance to programs on mitigations. Categorizing and characterizing risks into discrete levels and, scoring them relative to impact of exploitation is recommended.

There is a growing concern that DoD systems based on commercial chips might have security vulnerabilities that adversaries could exploit even when those vulnerabilities were not intentionally introduced.[11] Security concerns with emerging non-DoD applications, such as consumer IoT, has the potential to limit its acceptance and growth.[12] Semiconductor companies will be likely to address security issues to continue access to the IoT related market, reported at $800B this year (2017), representing a nearly 15% increase over last year.[13]

These adjacent non-defense industries are organizing efforts to address their needs for security (e.g., IoT, automotive, etc.), giving DoD an opportunity to join the dialog with the commercial semiconductor companies, or risk decreasing influence if the effort results in new standards and practices that address industry concerns outside DoD's interests. ***Well-funded and motivated industries may be successful in gaining concessions from the chip industry to address security concerns that DoD alone cannot achieve. Yet, DoD's unique security perspective can be a valuable voice in the dialog with semiconductor companies.***

[11] Defense Science Board Task Force on Cyber Supply Chain, Executive Summary, April 2017 (http://www.acq.osd.mil/dsb/reports/2010s/DSBCyberSupplyChain_ExecSummary_Distribution_A.PDF)
[12] Defense Science Board Task Force on Cyber Supply Chain, Executive Summary, April 2017 (http://www.acq.osd.mil/dsb/reports/2010s/DSBCyberSupplyChain_ExecSummary_Distribution_A.PDF)
[13] Natalie Gagliordi, "IoT spending to surpass $800 billion in 2017, led by hardware: IDC" (http://www.zdnet.com/article/iot-spending-to-surpass-800-billion-in-2017-led-by-hardware-idc/)

6 SUMMARY

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 in defense systems and assuring long-term availability of spare parts for long-lived defense systems is a challenge that is increasingly difficult as the life-cycle of chip technologies.[14]

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. As it is now, there are no methods for assessing security status of catalog microelectronics intended for critical roles in defense systems. Team 3 believes that it is possible to develop approaches that can provide assurances about catalog parts for use in some application areas. There are physical and functional verification techniques and perhaps design information can be obtained and scrutinized, among other techniques that can provide assurances. Team 3 acknowledges that establishing the criteria and metrics for security at the chip level is difficult and that there will likely be disagreements even in defining categories. ***But, ignoring the challenges of characterizing the security in using commercial microelectronics is a poor alternative to undertaking this difficult task.***

Commercial microelectronic components being considered for use in defense systems should be assessed for inherent trust and assurance properties as part of the selection process. With that insight, a program can determine the risk associated with those commercial components and make an informed decision about using those components and if additional buyer actions further reduce the risk associated with their use. Other implementations of risk management frameworks and risk-based approaches have led to levels or categorizations that will require expert debate to establish but can provide a better solution for the DoD over the long-term.

Commercial catalog components come without any evidence of meeting any defense specific trust or assurance requirements, but visibility into commercial practices can provide for some level of characterization of the trust and assurance. Adherence to standards and using volume

[14] Sally Cole, "Managing COTS Obsolescence for Military Systems" (http://mil-embedded.com/articles/managing-cots-obsolescence-military-systems/)

manufactured components has advantages and disadvantages; no general mapping existing for security or trust status. Developing a tiered methodology for assessing "Trusted Readiness" may be a starting point, followed by the additional controls or practices needed to establish a solid consensus approach.

DoD should collaborate and maintain a good working relationship with the merchant suppliers so that additional quality measures can be requested when necessary along with information or evidence of practices that support trustworthiness. Nevertheless, it is unlikely that DoD can dictate terms to merchant commercial suppliers with any degree of success (nor would DoD want to). Finally, partnering with other non-Government entities and industries with analogous security concerns could give a greater voice and leverage to DoD by increasing aggregation from various entities to address availability and security concerns. Examples of industries with analogous security concerns include critical infrastructure, medical/health, banking, automobile, cloud computing, and IoT.

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

1. 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.
2. 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.
3. With vendor participation, the DMEA Category II criteria could be used for an additional level of trust above the basic best commercial practice.