THE GUIDEBOOK ON TRUST

HOW TO PROCURE TRUSTED ASICS FROM ACCREDITED SOURCES

DISCLAIMER: This Guidebook is intended to assist stakeholders seeking to understand implementation of the Trusted Accredited supplier program and is not a substitute for stakeholder's seeking their own legal counsel to comply with legal requirements. Neither the TSSG nor its member companies are responsible for the interpretations expressed in this Guidebook.

CONTENTS

1. INTRODUCTION

This document seeks to guide those who would like to know how to specify and purchase Trusted components within DoD or security-sensitive electronics. It outlines the scope of products and services that can be obtained under the current program of DMEA accreditation as well as options within the current program. Finally, it guides interested parties to other sources of information relevant to lowering risk and increasing security within electronic systems.

The Trusted Supplier Steering Group (TSSG), a self-formed group of micro-electronics industry companies who are accredited by the DMEA to provide custom electronics to US DoD and their contractors and suppliers, recognized that significant gaps exist between DoD published guidance and current utilization of the Trusted Accredited suppliers for custom chips. In addition, questions arising from numerous enquiries to Trusted Suppliers within industry indicate that the information seekers and decision makers do not always fully understand why nor how to specify or purchase Trusted electronics.

Typical questions include:

- What are the requirements for using Trusted microelectronics?
- What is the benefit of using Trusted Suppliers??
- What types of products and services can I buy from Trusted Suppliers?
- What do the different categories mean and which do I need?
- Is there a premium for buying Trusted?

Because the DMEA and other DoD-related entities must be careful in their guidance to industry, the answers to these questions are not always readily available. In addition, as the combined and amorphous combination of industry, government and academia continues to identify new risks and new mitigations to those risks, the answers may change more rapidly than can be communicated solely by official government sources.

For these reasons, this guidebook is being made available as an informal and unofficial guide to those looking for the answers and who must navigate a rapidly changing world of electronics, risks, and mitigations to those risks as they develop electronics-based advanced systems.

2. TARGET BENEFICIARIES OF GUIDEBOOK

This guidebook may be particularly helpful to developers of electronic systems for DoD and critical infrastructure who need to comply with government guidelines while creating systems which are safe for end-users in their final market. Both small and large businesses develop DoD systems but the different personnel and roles within large prime contractors explain how many of larger entities typically divide their organizations into functional units – units which are then matrixed together for specific customer programs. Within these functional units (which may vary widely by company), there are at least four types of individuals that may have a need for this information and guidance: 1) **Program Office personnel** responsible for working with customers to define and manage programs; 2) **Sub-Contract Supply Chain and Material Program Managers** responsible for flowing down the rules and guidelines from the customer so that system integrity is held throughout the supply chain; 3) **Engineering Teams** responsible for the details of each electronics-based system; and 4) **Systems Security Engineers** responsible for the assurance of the design integrity and security.

Program Office personnel: The customer-facing functional units whose primary job is to work with customers to define and manage programs are often the front line in the interpretation of rules (FARS, DFARS), DoD guidelines, which when combined with the architectural demands of the target system (power, performance, size, etc.) create the outlines of the program. Cost and schedule trade-offs are managed and negotiated from the inception of the program through to end-of-life. For this reason, it is very important that any premiums that are necessary to protect the system and/or to meet the DoD rules and guidelines be understood in full. Whether these personnel understand, at the time of budget creation, which components will require custom chips may be an important factor in their ability to correctly predict cost and schedule. Also, correct application of the definition of CPI by the customer and prime will have an impact on which sub-systems required a Trusted flow.

Sub-Contract Supply Chain Managers: As a critical part of any large organization, the management of suppliers and supply chains is often part of the purchasing and/or components engineering functional units, which then often report to the finance part of the management team. In today's disaggregated world, no single company can build a complete system by itself from raw materials. The role of this group is critical because it ensures that all of the quality, reliability and engineering standards of the entire sub-contracted supply chain meet the standards of the prime at a reasonable cost. A significant aspect of this responsibility is the flow down the rules and guidelines from the customer so that system integrity is held throughout the supply chain.

Engineering: Often organized into skill set by first level managers and then divisions based on product lines, engineering teams are formed for each program (across the matrix) to architect the details of each electronics-based system. It is this group that is often tasked with the "trade studies" or "trades" which look into the feasibility and cost of each sub-system. Because there

is an often tedious aspect to collecting the data from possible component suppliers and delivering that to a spreadsheet for comparison and roll-up, many trade studies efforts will utilize the least experienced members of the team and it is a good learning experience for them as well. For this reason, engineering organizations may have the need for these guidelines on Trusted at many levels of seniority.

Systems Security Engineers: These engineers are typically part of the engineering functional unit and are some of the most senior engineers. Their responsibility is the assurance of the design integrity and security which means close management of sub-contractor process and identification of risks within their purview, whether that is at a system, board, or chip level.

3. RISKS TO ELECTRONICS-BASED SYSTEMS

Systems developers have a wide range of threats to the integrity of their systems, their core assets, and most critically – the ability of their customers to have confidence in their products. Everyone understands that hackers can get in to software, steal data and make unseen changes. All of this potential damage, and more, can happen to the underlying electronics as well. There are three major categories of risk, each with possible motivations of money or military advantage:

Infiltration: During every step of integrated circuit development, manufacturing, packaging and test – malicious or destructive changes can be inserted or introduced. This infiltration can be performed by employees, sub-contractors, or remote agents that gain access to systems with inadequate protection.

Exfiltration: Similarly, during every step of IC development, etc. – exfiltration is the loss (theft) of the some or all of the IC information – information that can be used to recreate or defeat the chip's purpose in its target system. This can also result in imitation or counterfeit versions that may find their way into target systems.

Supply Chain Disruption: Should a key supplier (think unique or sole supplier) of the long necessary chain of suppliers required for chip development become unavailable or become compromised by offshore purchase or insider threat or other disqualification of a supplier, systems can be shut down with little recourse.

In summary, electronics and the necessary long chain of supply that makes them possible are vulnerable to risks that can have major impacts on systems in development and in the field. Readers who are in charge of protecting their systems should understand the details of risks and much has been researched and written on the subject (see references in More Information for a few links)

Entire systems can be brought down with a single unauthorized change of a transistor or the loss of a key supplier.

4. MITIGATING RISK FOR ICS: ASSURE "CHAIN OF CUSTODY"

When systems companies need to acquire ICs from suppliers, whether custom or not, they should ask themselves "Who has had access to this IC during its design, manufacturing, and post-production phases?" One of the most important ways to assure Chain of Custody is to utilize a Trusted Supplier who has been accredited to provide this assurance. As outlined below, critical DoD circuits require the use of Trusted Suppliers and Processes but astute systems developers outside the policy requirements will consider Trusted Suppliers and their assurances because they share the same risks and impacts to their systems.

5. HISTORY AND REASON FOR TRUST ACCREDITATION

In the late 1990's many integrated circuit manufacturers (foundries) were moving offshore and concern was growing about maintaining domestic options. The Trusted Foundry Program was initiated in 2003 to ensure that mission-critical national defense systems have access to leading edge integrated circuits and it is administered and managed by the DoD Defense Microelectronics Activity (DMEA).

In 2005 the Defense Science Board issued a report which raised the possibility that *"Trojan horses"* and other unauthorized design inclusions might appear in unclassified integrated circuits used in military applications, or that subtle shifts in process parameters or layout line spacing might drastically shorten the lives of components. The DSB concluded that "*for the DOD's strategy of information superiority to remain viable, the Department requires: Trusted and assured supplies of integrated circuit (IC) components ….*" and recommended steps to plan the size and scope of the trusted program.[1]

In 2007, the Program was broadened to include companies that cover the entire microelectronics supply chain and an accreditation process was launched to ensure these suppliers meet Trusted criteria as established by the Trusted Foundry Program Management. These Trusted Suppliers are certified to provide state-of-the-practice services for new and legacy integrated circuits.

It is important to note that this program has been initially centered on the specific need for custom chips, which are unique to specific programs and, as is detailed below in the Risks section, they are more vulnerable AND more important to protect. The supply chain for other electronics such as FPGAs, standard product ICs, and PCBs, and other components differ and other approaches to creating secure supply chains are currently (2017) being developed and considered for standards. These concepts and efforts are outlined in the New Developments section below.

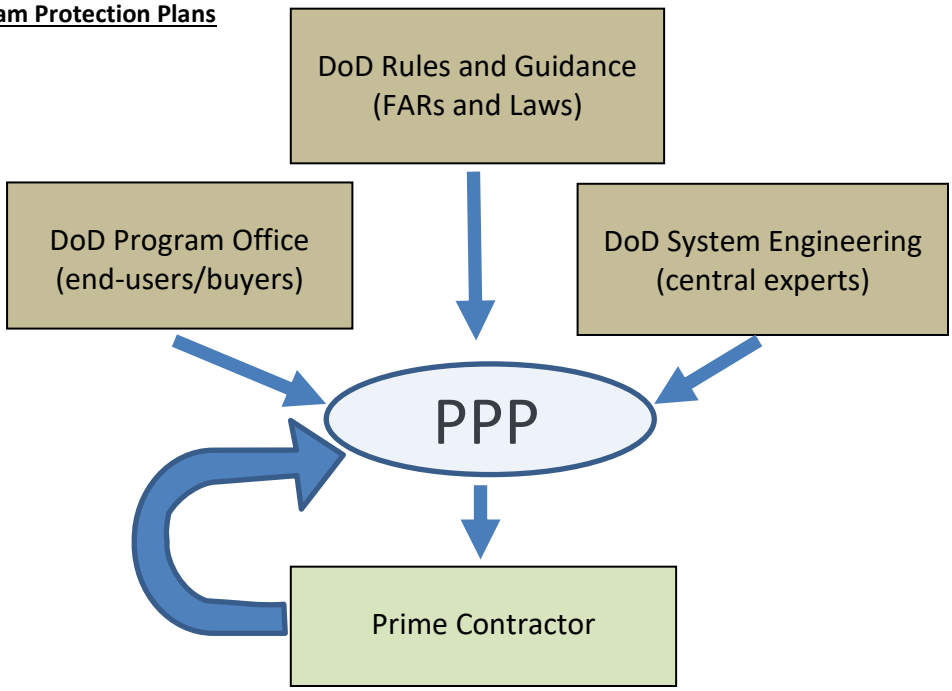
This document, therefore, primarily concerns itself with how (and why) systems developers should protect their custom chips by utilizing Accredited Trusted suppliers and where they can turn for additional information on the process.

---

[1] *Defense Science board Task Force on High Performance Microchip Supply, February 2005,* *http://www.acq.osd.mil/dsb/reports/ADA435563.pdf*

6. HOW DOD SYSTEMS WITH ELECTRONICS ARE PROTECTED BY TRUST

PPP: Program Protection Plans



Program protection planning (PPP) is a step-by-step analytical process to identify and analyze threats, determine program vulnerabilities, assess the risks and apply countermeasures to the system being procured. The PPP is applicable to all program/system developers, subcontractors, and operational users of the program and is updated throughout the life cycle. It is created by the DoD stakeholders (Program Office and System Engineering) utilizing expertise and input from the Prime Contractor. Of the many important jobs that this team has, apart from applying the rules and guidance (in both the written "letter of the law" as well as the intent behind the rules) is identification of "CPI[2]" (Critical Program Information) which is the aspect of the program requiring special attention and protection. Please refer to www.acq.osd.mil/se/docs/**PPP-Outline-and-Guidance-v1-July2011**.pdf for additional information on Program Protection Plans.

> Key Takeaway: Understand the rules and what is designated as "CPI" to navigate which components needs to use Trusted Electronics

[2] CPI: U.S. capability elements that contribute to the warfighters' technical advantage, which if compromised, undermines U.S. military preeminence. U.S. capability elements may include, but are not limited to, software algorithms and specific hardware residing on the system, its training equipment, or maintenance support equipment. See DoD Instruction 5200.39

7. RULES, GUIDANCE AND FARS DIRECT USE OF TRUSTED ELECTRONICS

There are numerous published instructions, rules, and guidelines that provide system developers with information relative to electronics. Within this set of rules, the one most applicable to ASICs - currently the main concern of the Trusted Supplier Accreditation Process (and these guidelines for that reason), is DoDI 5200.44: Protection of Mission Critical Functions to Achieve Trusted Systems and Networks. And within that instruction, the applicable paragraph reads:

> *"In applicable systems, integrated circuit-related products and services shall be procured from a trusted supplier using trusted processes accredited by the Defense Microelectronics Activity (DMEA) when they are custom-designed, custom-manufactured, or tailored for a specific DoD military end use (generally referred to as application-specific integrated circuits (ASIC))."*

It is worth noting that in an August 2016 update to 5200.44, the applicability of the instruction was amended to *include spare or replacement parts* used in mission critical functions and critical components.

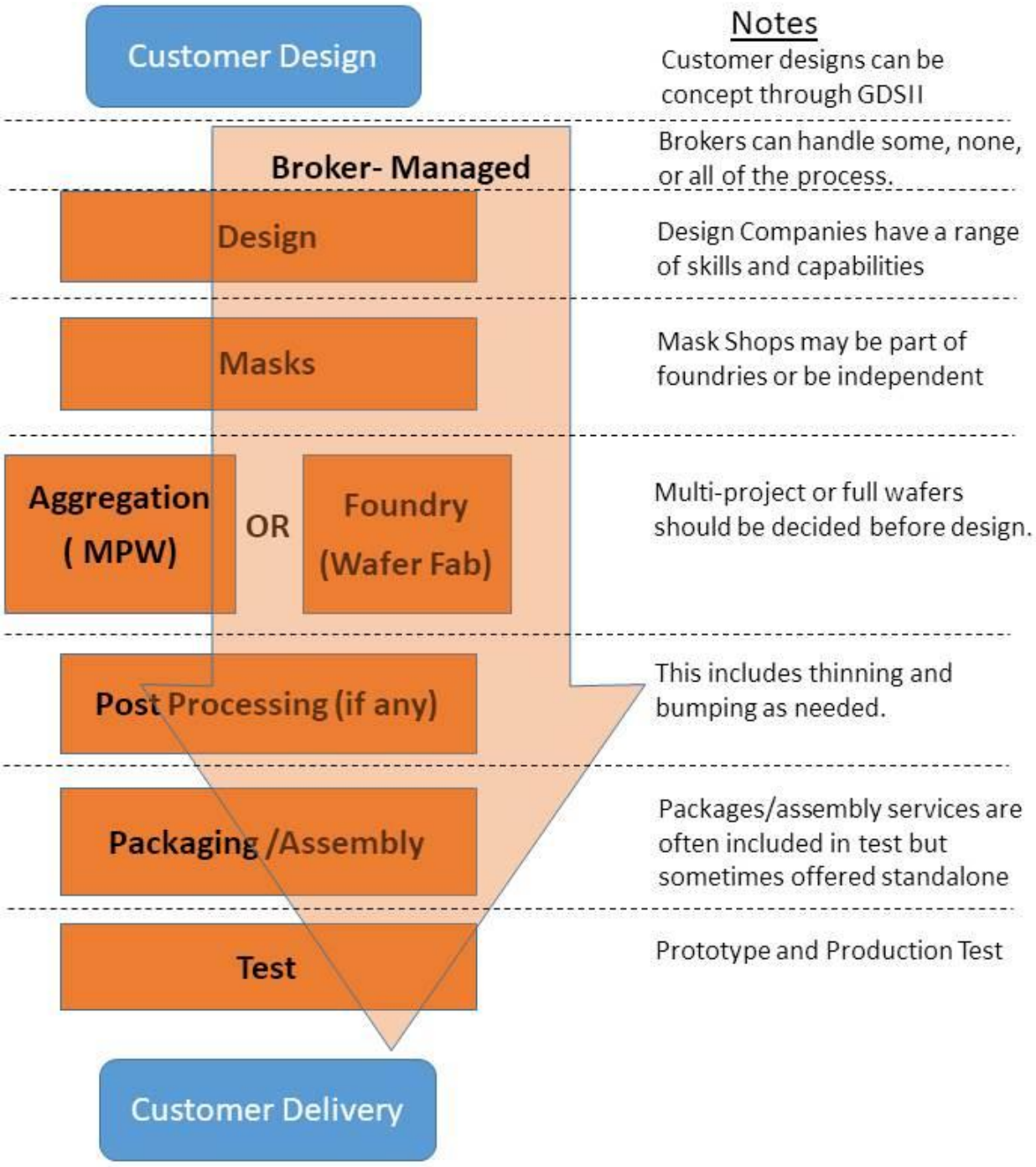
Additional information, rules, links and presentations can be found at the ODASD Systems Engineering web site. But the conclusion is that if your system is designated "CPI", then you must use a Trusted process and one of these suppliers for ASICs: DMEA Trusted Accredited Suppliers.

8. UNDERSTANDING THE COMPANIES AND OPTIONS IN A TRUSTED FLOW

As you will see in the flowchart on the next page, buyers of Trusted ASICs have options regarding whether to go to one company or entity to manage the whole process (accredited brokers) or select and manage the different specialties themselves. Each accreditation type is equivalent to the specialties that exist within the industry and the right choice may be a different company at each step or choosing companies or entities that have the ability to offer several steps. The choice will likely come down to the specifics of the chip technology needed (process choice) and the state of the design rather than business issues but the competitive landscape that offers alternatives also creates some complexity. Talking to several accredited design and broker companies will likely flesh out the available options for specific buyers and their designs.

One source of confusion for Trusted ASIC buyers can be that the DMEA, the government agency that accredits and maintains the supplier base in conjunction with the DSS who performs the oversight of clearances and classifications, also provides almost all of the services shown in the chart show on the following page. They maintain a non-exclusive agreement with Global Foundries for access to some of their processes and TAPO (Trusted Access Program Office) is one gateway to those processes. However, the accredited brokers can also offer access to those processes and may provide different services either themselves or through other accredited parties. Any confusion about DMEA/TAPO offerings can also be sorted out by talking to the TAPO team as well as an accredited broker or design company.

Flowchart of Accredited ASIC Processes



9. BUYING TRUSTED ELECTRONICS – A STEP BY STEP PROCESS

The steps shown below are somewhat simplified but they should help create an understanding of the key decisions in the process. System developers and primes maintain experts, system security personnel and knowledge bases within their corporate staff that may help answer the questions posed in these steps:

1) **Confirm that the target is an ASIC:** While efforts are underway to expand Trust to other forms of electronics, the requirements and focus has been ONLY on ASICs. Proceed to Step #2 if your electronics include a custom chip or ASIC.
2) **Check Classification Level:** Accredited suppliers are cleared by the DSS to develop classified devices; this is one of the key benefits of the accreditation process for DoD and Systems Developers. In that case, you will need to utilize Category 1A[3] suppliers and flows and follow your DD 254[4]. Proceed to Step #5 if your program is classified.
3) **For Unclassified DoD Programs – the Key Questions are CPI and ITAR:** Many unclassified programs will have CPI designation on their electronics and thus be required to utilize Trusted Suppliers for that portion of their ASICs. Because a Trusted Flow is essentially the same as a Classified Secret Flow, this can lead to confusion since the program does not typically issue a DD 254 which guides subcontract management and engineering personnel in data management. However, the tighter restrictions are important as each step of the ASIC design and development and manufacture and test and packaging are often different companies and therefore risks are higher than would exist natively within the systems developer or prime. Note, however that the following section (Section 10) of this guidebook deals with some of the gray areas related to Trusted Unclassified programs. Either way, ITAR restrictions which are quite common for DoD programs, should be understood before taking the next step of communicating with suppliers. Proceed to Step #5 if your electronics are or should be designated CPI.
4) **Non-DoD and Non-CPI Programs should use Trusted Companies**: The risks that exist for CPI electronics or classified programs are still there for ASICs done outside of those worlds. No company can long withstand the wholesale loss or copying of their intellectual property and for some companies, a breach or failure to protect their customers or their customers' data can mean losses in the millions or billions. Ensuring chain of custody and peace of mind within the highly disaggregated world of electronics is an important goal for all electronics developers. As a result, system developers often turn to Trusted Suppliers for Non-Trusted Flows simply because

[3] DMEA utilizes Categories to show levels of Accreditation and for different types of devices. While most Accredited ASIC suppliers are Category 1A, there are some Category 1B suppliers that may be appropriate for unclassified but Trusted devices. Refer to the DMEA or those suppliers for more information.

[4] The Federal Acquisition Regulation (FAR) requires that a DD Form 254 be incorporated in each classified contract. The DD Form 254 provides to the contractor (or a subcontractor) the security requirements and the classification guidance that would be necessary to perform on a classified contract.

they natively offer a far more secure supply chain even when they utilize their standard flows. Accreditation by the DMEA tightens process and awareness across the board at Trusted Suppliers, which in turn, enables customers to select purchasing options based on their perception of risk. In this case, potential customers should tailor the risk mitigations and options which each supplier can offer for a cost/risk balance that meets the perceived goals. Proceed to Step #5 if your non-DoD system needs the best protection available.

5) **Contact a Trusted Supplier to Get Started**: Upon determining that you would like to utilize a Trusted Supplier or Trusted Flow, consult with one or more of these: DMEA Trusted Accredited Suppliers to begin the source selection process. Here you will find Trusted services and contact information for each DMEA accredited supplier. Determining hand-off points of design databases from developer to Trusted Supplier will be an important early decision point but each supplier can help you understand the trade-offs and options. Your entry point will likely be a supplier accredited for Design (to help prepare for mask development) or a supplier accredited as a Broker (who can manage the range of Trusted Suppliers for you). Understanding the strengths and capabilities of all of your potential suppliers will be important as you navigate the choices that make sense for your program. Another important point to consider is that unless you work with a broker or supplier with a full range of accreditation for all services, you will need to manage the hand-off points between services providers and insure a Trusted handling that is equivalent to Classified. Experienced ASIC buyers will also understand that different foundries and suppliers have different capabilities and costs that must also match the system and budget requirements of the system – finding the best match may require talking to several suppliers. DMEA may also be contacted to assist potential buyers of Trusted components, they are also able to act as brokers and have their own services and foundries as well.

10. IMPORTANT EXCEPTIONS, ADDITIONS, AND UNPUBLISHED GRAY AREAS

TRUSTED – UNCLASSIFIED

Each Trusted Supplier is accredited by the DMEA to perform all of its steps at a SECRET level of classification and the DMEA works with the DSS to insure that these suppliers can operate at that level. The Trusted Foundry program insures that capacity is kept in place during periods of non-use. In addition, most documentation and essentially all assumptions are based on receiving classified inputs, working within the NISPOM guidelines for SECRET, and then delivering outputs at that same level. However, many programs that may require TRUSTED are not classified (or are not classified at the detailed design level) and therefore do not have design data, documentation, and infrastructure to support moving into a classified process. Equally important, there are costs associated with the "closed room" nature of classified efforts that are not always within the budget for some of these programs which may be designated ITAR or simply need ASICs for CPI-designated electronics. The solution for these programs is often: Trusted Unclassified. This is an undocumented space because government oversight and rules cannot fully dictate the correct trade-offs within the supply chain when something less than SECRET is assumed. For this reason, System Security Engineers and those responsible generally for the security of data and design information within the supply chain have to be very careful when deciding which functions, which exceptions, and which processes should operate outside of a closed room, outside of a SECRET solution. The important first step is to choose an accredited Trusted supplier and then use their input and informed knowledge of the risks to make decisions when choosing Trusted Unclassified. Some suppliers may require the creation of a DD 254 to utilize their Trusted flows and others may have specific guidance on which aspects of the process will remain in a classified flow and which will not. Buyers can be assured that each supplier will be able to protect their customer's data and will provide transparency as to any exceptions and trade-offs within their process. It may go without saying but one of the largest risks within any supply chain is the robustness of their communications and connections to and through the internet. Looking at compliance to standards such as NIST 800-171 should provide significant insight as to the infiltration/exfiltration risks as compared to the buyer's own systems and networks.

UNTRUSTED IP SOURCES

When creating electronics-based system, a significant portion of Intellectual Property (IP) from the outside world must be incorporated. Like the nuts and bolts of the mechanical world, quality and reliability must be measured and quantified – to the extent possible. It is this last caveat that creates concern for complex IP that will be located at the heart of a system: how can you be sure that the IP can be trusted completely. For most commercially available IP that is used across the industry, there is small probability of a problem and this is similar to the very small probability that a standard COTS device has undocumented backdoors or failure modes. But for critical systems, this non-zero risk must be included in the thought process. Moreover, since IP within custom chips increasingly comes from a wide spectrum of companies across the globe – these hardware (and software) building blocks must be seen as an element of risk. Risk not easily quantified but mitigated at least partially by looking closely at the origin and component of each source of intellectual property.

11. NEW DEVELOPMENTS AND EFFORTS TO EXPAND AND ADD TO TRUST

Groups within the government and industry as well as coalitions between them (including organizations such as NDIA) are constantly meeting and discussing the best ways to meet a growing list of known and unknown risks. Readers should understand that no one program or solution will perfectly mitigate all risks – so there are two necessary tasks: 1) Understand the risks and 2) Invest in an understanding of the current best practices and rules in place to mitigate risks. This guidebook treats these two subjects in a very cursory fashion and groups such as DARPA and many industry experts/companies are creating solutions that solve unique aspects of risk such as counterfeit detection, chain of custody assurance, etc. These solutions should be viewed as an ever-expanding but imperfect web of protection against an ever-expanding set of risks. Education on the latest and greatest risks and mitigations is critical – talk to a Trusted Supplier, consult with a System Security Expert, and get involved if possible with the many efforts to ensure safe electronics and systems.

12. LINKS TO MORE INFORMATION

www.acq.osd.mil/se/docs/**PPP-Outline-and-Guidance-v1-July2011**.pdf

DMEA Trusted Accredited Suppliers

ODASD Systems Engineering

DoDI 5200.44

DoD Instruction 5200.39, Critical Program Information (CPI) Identification and Protection Within Research, Development, Test, and Evaluation (RDT&E), May 28, 2015

www.definedbusiness.com/files/pdf/casestudies/microelectronics_threat_brochure.pdf

VIB-Marrujo.pdf

0930 - Harzstark - QML vs TRUST.pdf

Eisenhower School - Spring 2017 Industry Study Industry Report Electronics –

GAO Report TRUSTED DEFENSE MICROELECTRONICS Future Access and Capabilities Are Uncertain

Department of Defense (DoD) Trusted Microelectronics

13. DISPOSITION AND DISTRIBUTION NOTES

DISPOSITION AND FEEDBACK METHOD

This is the initial release of the Trusted Guidebook: Ver2017Q4.01. It is primarily intended to be provided in electronic format in PDF format. Versions will be made available and published as content is updated. To request updates and to provide feedback, contact:

Jim Gobes: jgobes@intrinsix.com (508) 658-7658

DISTRIBUTION METHODS IDENTIFIED TO DATE:

- Emailed Direct from Trusted Suppliers and others on demand
- Available for Download from TSSG-approved sites
- NDIA website (as permitted)