Trusted Microelectronics Workshop:

"Trusted Microelectronics: The Future Landscape"

August 25, 2015
Hosted by the Institute for Defense Analyses (IDA) and the
National Defense Industry Association (NDIA) Event 5290

Acknowledgments

This workshop came together with the help of a number of important people. Ms. Britt Bommelje and Ms. Rebecca Danahy of the NDIA did a great job organizing and hosting the event. Dr. Brian Cohen and the IDA staff are thanked for providing a wonderful site to hold this workshop. Thanks to the keynote speaker Mr. Robert Gold, Director, Engineering Enterprise, Office Deputy Assistant Secretary of Defense (ODASD), Systems Engineering (SE), who spoke about the future landscape of trusted microelectronics and to Mr. David Meshel of Aerospace Corporation for speaking about efforts by the space community to obtain trusted microelectronics from untrusted sources. Many thanks to the panel members that included Mr. Gold, Mr. Meshel, Mr. Don Davidson, Office of the DoD Chief Information Officer, Mr. Ray Shanahan, ODASD(SE), Ms. Melinda Woods, ODASD, Manufacturing and Industrial Base Policy (MIBP), and Mr. Jeff Krieg, National Security Agency (NSA), co-chair of the Department of Defense (DoD) Joint Federated Assurance Center (JFAC) Hardware Assurance Working Group. Once again, attendee participation was key to the workshop's success, so thanks to the many participants who were very active in the event discussions. Finally, the efforts of Dr. Brian Cohen (IDA), Mr. Sydney Pope, Decisive Analytics Corporation (DAC), and Ms. Catherine Ortiz, Defined Business Solutions, are appreciated for organizing the event and ensuring that the workshop ran smoothly.

Contents

1. Introduction

The NDIA Trusted Microelectronics Workshop series was launched in 2013 to provide an open forum for government and industry to discuss microelectronics supply and security issues related to defense and national security systems. The initial workshop held in June 2013 explored how to make the Department of Defense (DoD) Instruction 5200.44 a success.[1] The report from that meeting recorded a strong desire by the participants to follow up that first workshop with similar events.[2]

A subsequent meeting was held in January 2014 with the theme of "Trusted Microelectronics for Systems Security."[3] The report from that meeting discussed a number of areas identified for further discussion including opportunities for managing supply chain risk beyond Application Specific Integrated Circuits (ASICs) and opportunities for cost-effectively leveraging industrial capabilities.[4]

In August 2014, the third Trusted Microelectronics Workshop explored the overlap between the requirements of safety, quality, and security in aerospace and defense systems.[5] The report from that meeting included good approaches discussed by the audience on how to leverage existing quality and safety disciplines to address supply chain security risks.[6]

The fourth Trusted Microelectronics Workshop,[7] held in February 2015, was designed to consider hardware assurance challenges in a system's sustainment phase, as components are more difficult to get from the original suppliers. The report from that workshop included discussion on how sustainment managers and representatives from the Diminishing Manufacturing Sources and Material Suppliers (DMSMS) community are using trusted and trustworthy suppliers to mitigate electronic component risks later in the

---

[1] NDIA Event 3180 - Trusted Microelectronics Workshop

[2] Trusted Microelectronics Workshop: "Making 5200.44 a Success," Report on the NDIA Workshop 3180, June 28, 2013

[3] NDIA Event 4290 - Trusted Microelectronics Meeting

[4] Trusted Microelectronics Workshop: Trusted Microelectronics for Systems Security, Report on the NDIA Workshop 4290, January 15, 2014

[5] NDIA Event 487E - Trusted Microelectronics Meeting

[6] Trusted Microelectronics Workshop: "Connecting Safety, Quality and Security: The Benefits of Trusted Microelectronics," NDIA, August 21, 2014.

[7] NDIA Event 587D - Trusted Microelectronics Workshop

lifecycle.[8] The audience asked for better definition of the DMSMS problem, identification of stakeholders, and development of the process to get systems engineers and supply chain managers to address security risks early in the component selection process.

The most recent Trusted Microelectronics Workshop, held on August 25, 2015, looked to the future. Specifically, how the DoD could satisfy the need for trusted microelectronics in an increasingly globalized integrated circuit industrial base. With a theme of Trusted Microelectronics: The Future Landscape, the workshop was advertised publicly on the NDIA website and key groups of government and industry were invited to participate as follows:

"NDIA is pleased to offer our fifth workshop designed to identify ways in which trusted microelectronics can contribute to greater systems security and information assurance. With participation from both Government and Industry, our half-day workshops have provided an effective forum for direct discussions of the challenges faced by policy makers, program managers, systems developers, and supply chain managers.

At this workshop Government experts will discuss the work being done to ensure:

- Government programs have choices for leading edge microelectronics technologies that are trustable
- State-of-the-art technologies critical to national defense programs are available from domestic sources
- R&D in technologies that address trust are part of the overall microelectronics strategy

Mr. Robert Gold, Director, Engineering Enterprise ODASD(SE) will provide the keynote address. As a member of the Senior Executive Service, Mr. Gold is responsible for systems engineering-related policy and guidance, specialty engineering, engineering tools and environments, hardware and software assurance, and defense standardization. His specialty engineering responsibilities include reliability and maintainability, system safety, manufacturing, human systems integration, and the DoD Value Engineering program.

Mr. David Meshel will present National Reconnaissance Office's (NRO's) best practices to procure trustable components from untrusted sources. A panel of Government experts has been assembled to discuss component protection options for ASICs and beyond.

---

[8] Trusted Microelectronics Workshop: "Hardware Assurance for the Lifecycle: The Benefits of Trusted Microelectronics," NDIA, February 26, 2015.

Our workshops are designed to be truly interactive with full participant engagement. Please join us to learn about the Department's microelectronics strategy and to add your voice to the conversation.

Who should attend: Government and Industry program managers, systems engineers and developers, microelectronics designers, supply chain and sustainment officials, purchasing and procurement professionals, product managers and operations analysts."

Dr. Brian Cohen, an IDA Research Staff Member, opened the workshop with an introduction to the day's theme of exploring issues revolving around the future for trusted microelectronics. Dr. Cohen stated that the landscape for microelectronics continues to migrate away from U.S. soil. Because of this shift, the Department is developing strategies, guidelines, and new policies to protect defense and national security systems with increasingly complex supply chains.

Mr. Robert Gold, Director, Engineering Enterprise, ODASD(SE), provided the keynote address and expressed his appreciation for the opportunity to engage thought leaders on this topic.

Following Mr. Gold's presentation, Mr. Sydney Pope, a DAC Systems Security Specialist, moderated a discussion on the leverage points that Mr. Gold introduced in his keynote.

After a break, we heard from Mr. David Meshel, a Senior Project Leader with Aerospace Corporation, who presented work done for the NRO to secure their supply chain, entitled "Procuring Trustable Components from Untrusted Sources."

The workshop continued with a panel of microelectronics experts. Dr. Cohen moderated the discussion during which the panelists addressed questions both from the moderator and from the attendees. The full agenda is shown in Appendix A. The keynote presentation from Mr. Gold is in Appendix B and Mr. Meshel's presentation is not available for publication but his contact information is provided in Appendix C. Anyone interested in a copy of his presentation should contact Mr. Meshel. The registration roster is provided in 3.Appendix D.

2. Minutes of the Workshop

On Tuesday, August 25, 2015, the NDIA sponsored a Trusted Microelectronics Workshop, with technical co-sponsorship by the Trusted Suppliers Steering Group, at the IDA, Alexandria, Virginia. Seventy-five individuals from government and industry attended. A copy of the Agenda is in Appendix A. The Workshop began at 8:30 a.m. and adjourned at 12:30 p.m.

Welcome

Dr. Brian Cohen, IDA Research Staff Member

Dr. Cohen kicked off the workshop by describing its goal and then introducing the keynote speaker, Mr. Robert Gold

A. Trusted Microelectronics: The Future Landscape

Mr. Robert Gold, ODASD(SE), Director, Engineering Enterprise

Mr. Gold started his presentation by stating that trust-related policies need to be informed by industry technical experts and he welcomes the opportunity to hear from the meeting attendees. His organization, DASD(SE)/Enterprise Engineering, takes a long-term view of supply chain technical and security requirements; addressing hardware assurance, anti-tamper, and counterfeit prevention along with foundational and crosscutting engineering activities, such as systems engineering, manufacturing and quality assurance.

In his office, he encourages managers to incorporate science and technology (S&T) into engineering thinking to fully leverage S&T investments. Mr. Gold stated that wholesale technology investment is needed to replenish capabilities and he welcomes ideas from outside the Pentagon and endorses greater collaboration with industry.

Mr. Gold described microelectronics malicious supply chain risk, and the evolving government response. The Department can no longer ensure hardware security with a compliance/checklist mentality. Program managers need to manage their systems from a mission-critical functionality perspective, while not losing sight of easy targets. He emphasized the need to look at easiest attack vectors, to include vulnerabilities that might be found in non-mission-critical functions that can be used to exploit or access mission-critical functionality.

As an example, Mr. Gold described how an adversary might target vulnerabilities in the cockpit electronics of a commercial aircraft, or, alternatively, the pilot and crew work scheduling software to impact crew availability. He cautioned that supply chain risks are more dependent on electronics and software than in the past. New technologies need to be designed with these emerging threats in mind, addressing both cybersecurity and supply chain trust issues.

ODASD(SE) continues to work on policy, guidance, and training, and to provide acquisition program assistance, addressing the mitigation of system security risk and is challenged to stay ahead of the threat in a dramatically constrained budgetary environment. At the same time, Defense Procurement Acquisition Policy (DPAP) is working to develop better acquisition guidance and is engaging industry in a dialog on their body of practice for supply chain security – what policies are effective and which ones are burdensome.

Mr. Gold stated that understanding commercial off-the-shelf (COTS) vendors' supply chain practice is critical as the Department seeks to engage more broadly with commercial markets. He described the attractiveness of using field-programmable gate arrays (FPGAs), as they are usually less expensive and easier to engineer than ASICs; but that those advantages come with increased downstream supply chain risks for which there is not yet a comprehensive solution.

The JFAC, chartered by the Deputy Secretary of Defense earlier this year, is managed from Mr. Gold's organization. Recent JFAC activities include the development of its concept of operations (CONOPS) and the conduct of a DoD-wide software and hardware assurance capability gap analysis, which is expected to be completed in fiscal year 2016.

Mr. Gold stated that weapon and information and computer technology systems are more complex than ever; containing thousands of parts with increasing dependence on automation. Much attention has been paid to counterfeit prevention, which is critical, but there needs to also be recognition that a bad part can be introduced into the supply chain for espionage as well as economic reasons. Either motivation can result in catastrophic consequences. Uniform detection and response is critical and all prevention, detection and response elements need to link together.

Today, the government has "cylinders of excellence" that address different elements of trust that need to be better integrated for greater impact. These entities should work together on issues, document the steps needed to mitigate risks, and come up with best practices. When consistencies emerge, policy can be developed around it. Enabling trust is not an issue that can be solved by developing a flow chart with step-by-step instructions, but can be better addressed by providing tangible guidance.

In summary, Mr. Gold cautioned against equating budget allocation to an issue's importance in the current environment. Government programs are looking at ways to protect all critical integrated circuits (ICs) throughout the lifecycle with a greater emphasis on risk-based processes and technology development in accordance with Department Trusted Systems and Networks policy.

In response to questions from the participants, Mr. Gold stated that current challenges include:

- Support for low volume microelectronics production.
- Developing methods for secure designs and post-fielding upgrades.
- Creating communities of interest for hardware assurance with supporting technical working groups to assist with working hard problems.

B. Open Discussion

Mr. Sydney Pope, DAC, Systems Security Engineering Expert

An open discussion was moderated by Mr. Sydney Pope, a ODASD(SE) support contractor.

Mr. Pope opened the discussion by asking, "Where do we have the greatest potential to succeed at developing the tangible guidance Mr. Gold mentioned? What do we focus on?" The participants suggested that the DoD would benefit from greater use of on-shore low volume foundries. Good support was voiced for greater investment in domestic integrated circuit capabilities.

Further discussion centered on working with academia like Vanderbilt University's Institute for Space and Defense Electronics (ISDE) and similar research centers. Concern was expressed about the existence of non-U.S. researchers in academia that could lead to intellectual property theft. However; there was general agreement that early stage involvement with academia is practical and can be efficient.

Mr. Pope followed with the question, "Do we need a spectrum of policies and mitigations to ensure our systems can be trusted?"

A general consensus was that:

- Domestic manufacturing strategies are needed to promote trust at the system level.
- Industry standards may be the most affordable approach, but can be less comprehensive than the risks demand.
- Trust and trustworthiness need to be enterprise-wide priorities rather than tasking program managers with a responsibility that could be better addressed at a higher

organizational level.

- DoD Program Protection Plans (PPPs) and risk-based management principles can be lost in programs where specific performance, budget and schedule concerns take priority.

The next discussion responded to Mr. Pope's question, "How do we address system-level trust with FPGAs?"

A lively discussion produced the general consensus that:

- Technology is making FPGAs more interesting to consider for defense systems but increases the need to ensure they can be trusted.
- Testing FPGAs for trust is difficult. Testing each component (chip, intellectual property) of an FPGA can be too resource-intensive (time and money) for a single program. Assessments need to be done in support of the enterprise and leveraged by programs consuming those components.
- Industry is looking at creating partnerships to develop trust design standards and verification protocols for FPGAs.
- Hybrid FPGAs are advancing, which could make them more powerful solutions than traditional components.

Finally, Mr. Pope asked, "How can we create trusted systems from untrusted parts? Can we have enough trust in individual suppliers or components to have trust in our systems?"

Relevant comments included:

- "Buying American" to a technically acceptable level of trust does not ensure there are no foreign parts, or that the component is secure.
- The ODASD(MIBP) is working to gain a better understanding of common concerns between industry and government that includes polling both to evaluate best practices.
- Microelectronics is well suited for government and industry collaboration and we need to understand how the government can invest to ensure domestic capability thrives.
- The challenge is to find a way to take everything known about the threats and implement supply chain mitigations to enable more secure systems.
- To promote a better understanding among program managers, a recommendation was made to develop a classified briefing for them that contain examples of malicious insertion, since they are ultimately responsible for delivering systems that protect against supply chain risks.

C. Procuring Trustable Components From Untrusted Sources

Mr. David Meshel, Aerospace Corporation Senior Project Leader, National Systems Group

Mr. David Meshel presented the work his team is doing for supply chain protections in NRO systems. He described the NRO's dependency on advanced microelectronics that is greater than many other defense systems and how the supply chain threat is increasing.

Mr. Meshel emphasized the role of the Space Quality Improvement Council (SQIC)'s Mission Assurance Improvement Workshops (MAIW) to successfully integrate supply chain management approaches and investigate areas for commonality between programs.

Their "Counterfeit Parts Prevention Strategies Guide" has contributed to zero counterfeit incidents since 2008. The Defense Acquisition Guidebook is routinely monitored to incorporate new requirements into this document.

The MAIW has published a new document to assist programs with microelectronics supply chain security and risk mitigation: "Countermeasures to Mitigate Malicious Attacks to ASICs and FPGAs Circuit Development." The document should be published in September 2015 and will be available to DoD and the industry contractor base.

The 2016 MAIW is being planned to develop a new guideline document that focuses on inspection and test methodologies for the detection of tampered microelectronics.

D. Panel Discussion: "Protection Options for ASICs and Beyond "

Dr. Brian Cohen moderated a panel of subject matter experts consisting of:

- Mr. Don Davidson, Deputy Director, Cybersecurity (CS) Lifecycle Risk Management and CS/Acquisition Integration in the Office of the Deputy DoD Chief Information Officer for Cybersecurity, DoD DCIO(CS)
- Mr. Robert Gold, Director, Engineering Enterprise, ODASD(SE)
- Mr. Jeff Krieg, Chief, Hardware Reverse Engineering, National Security Agency
- Mr. Dave Meshel, Senior Project Leader, National Systems Group, The Aerospace Corporation
- Ray Shanahan, Deputy Director, Anti-Tamper/Hardware Assurance, ODASD(SE)
- Ms. Melinda Woods, Assistant Director of Strategic Programs, ODASD(MIBP).

Dr. Cohen started the discussion with the question, "What are the protection options for products coming from the global industrial base? Some suggestions offered included:

- DASD(MIBP) is currently asking industry leaders for their best practices and industry is eager to figure out what Government wants. Confidence in parts and suppliers can be a competitive discriminator.
- It is hard to define standards for COTS products. The Department of Commerce white paper on cybersecurity standards has been released for public comment. Executive Order 13636 has a goal of improving cybersecurity through acquisition standards. General Services Administration (GSA) is looking to add best practices from these efforts to commercial contractors' schedules.
- The Department is increasing work with industry for testing and verification. This will enable greater insight to vendor intellectual property to make verification easier.
- We have an opportunity to combine trust with other qualifications to add trust in the requirements at the program start.
- Our past performance information retrieval system (PPIRS) has quality control criteria to allow automatic selection of part suppliers. There is potential to add trust to the criteria to evaluate insider threats in a way that is transparent and legally defendable.
- We are going more to using customized COTS microelectronics. COTS products can be used as a logical evolution of protection, from desktop to ruggedize and beyond.
- To be most effective, the JFAC's approach is to "acquire to verify" that buys the intellectual property with the system to prevent long and costly reverse engineering.

Dr. Cohen then asked, "Government buyers do not buy microelectronics directly. How can government priorities translate to industry practices?"

Comments included:

- Top-down policy is needed with bottom-up information sharing and best practices from industry.
- Industry is becoming more protective of their supply chain and continues to update their best practices. As a result of breaches that have been made public, industry has become more open about how they assure product integrity. For example, there is now greater care taken with the information that companies share with their supply chain partners. This increased attention provides an opportunity to collaborate to develop best practices.

- JFAC would like to promote information sharing between government and industry to allow more open conversations about vulnerabilities.
- Government should participate in companies' activities to coalesce requirements on trust from outside government, such as National Institute of Standards and Technology (NIST) supply chain risk management practices, Society of Automotive Engineers (SAE) anti-counterfeit and International Standards Organization (ISO) security standards.

Dr. Cohen's next question was, "Twenty companies supply 80% of microelectronics purchased by government. Where do we address trust? At each purchase, or once per vendor?" A range of suggestions and unresolved issues were offered, including:

- The path from policy to actual fielding of systems is difficult to navigate. Does the government understand to what extent trust can be built into defense systems?
- Developing robust engineering practices is at the core of trusted systems. We need to build in trust in early as possible, pre-Milestone A.
- We need to recognize that different leverage exists when the part being procured is a $40 FPGA or a $65K custom ASIC space part.
- There tends to be general guidelines versus specific "how-to." For example, the, The Open Group global consortium has published general guidelines for trust comparisons. These could be brought closer together through a risk-based approach using cooperative research and development agreements (CRADAs).
- It is hard to make security mitigations attractive to industry. Government needs to make the case for the investment in enhanced security. Have we looked at what other industries are doing and adopted what can be leveraged?
- We are able to quantify the costs of loss after the fact. If we can do so before loss, we can better describe the risk involved.
- Getting the Intelligence Community more involved would likely prove to help guide the adoption of tangible trust enhancing practices.

A participant asked if the Aerospace Corporation guidelines presented by Mr. Meshel would be incorporated into acquisition technical requirements. This led to the following discussion:

- The government is evaluating key performance parameters (KPP) for systems survivability. As the work progresses, the Aerospace guidelines will be included in new contracts, and, perhaps eventually, existing contracts.

- The Net-centric KPP, focused on interoperability, adds a cyber aspect, but programs have been hesitant to require specific industry standards because compliance may not be auditable.
- The NIST cybersecurity frameworks and Special Publication 800-161 have been generally referenced in contracts regarding cyber. It may be beneficial to work with SAE and other organizations.
- Systems security engineering has to adapt to the system's mission and make PPP and supply chain risk management sections reflect the proper level of controls.

A discussion on the importance of training and education was initiated from the participants, and it was generally agreed that:

- Educating contractors and Original Equipment Manufacturers (OEMs) on cyber policies should be a priority; especially with trusted design and systems security engineering. However, there is a risk of putting design approaches in universities.
- NSA has Centers of Academic Excellence at 180 universities that have been designated for cyber and information assurance, which can be used for training.
- National Network of Manufacturing Innovation Institutes (NNMII) may present a path for trust training and building expertise.
- The ManTech Program may be leveraged to increase trust through enhancing domestic capabilities and disciplines.

Dr. Cohen captured the essence of the workshop with the question, "How do we deal with a broader set of security issues – can we have mutually assured security?"

Summary statements and unanswered questions included:

- The government is challenged by the industry's view that cyber has nothing to do with hardware. We need to address this misconception before hardware assurance will be taken seriously by industry.
- Most of us want the technology without thinking about the risks.
- More investment is needed in both research and developing practices but we should not ignore the benefit of developing the political will. Government could be the leader with setting the agenda that companies can use to justify their investments.
- Industry organizations, such as the Semiconductor Industry Association (SIA) and Semiconductor Research Corporation (SRC), are developing new research agendas to help push security issues in addition to addressing workforce skills in both government and industry.

- "Let the industry take care of this" is not a great way to let security be developed. Government has a duty to learn and understand why and how security measures are being implemented.
- Attention needs to be put on how to better position ourselves when we need to respond and recover. We are now working to the left of the boom. We need to devote resources into recovering after an event.
- The microelectronics industry is evolving to a security-conscious market. Government has an opportunity and a responsibility to take advantage of this awareness to describe how security protections benefit everyone.

Dr. Cohen asked a final question, "Where do we go with the Trusted Microelectronics Workshops from here?" Comments included:

- We are missing the OEM contractors at these workshops, the ones that do the integrating and the buying of systems. They need to be involved in the trusted systems discussions and to weigh in on standards.
- Are there security experts in other industries who could provide insight to their experience and solutions?
- We would like to hear from the people who write the contracts to better understand that process.
- Do we have experts who can help differentiate between intentional "test points" versus malicious intent versus "stupid." Either way, a vulnerability is a vulnerability, but we could benefit from understanding the origination.
    - Full day workshops are easier to justify than half-day events for those who travel to attend since nearly one-third of the attendees came from outside the Washington DC area.

3. Summary

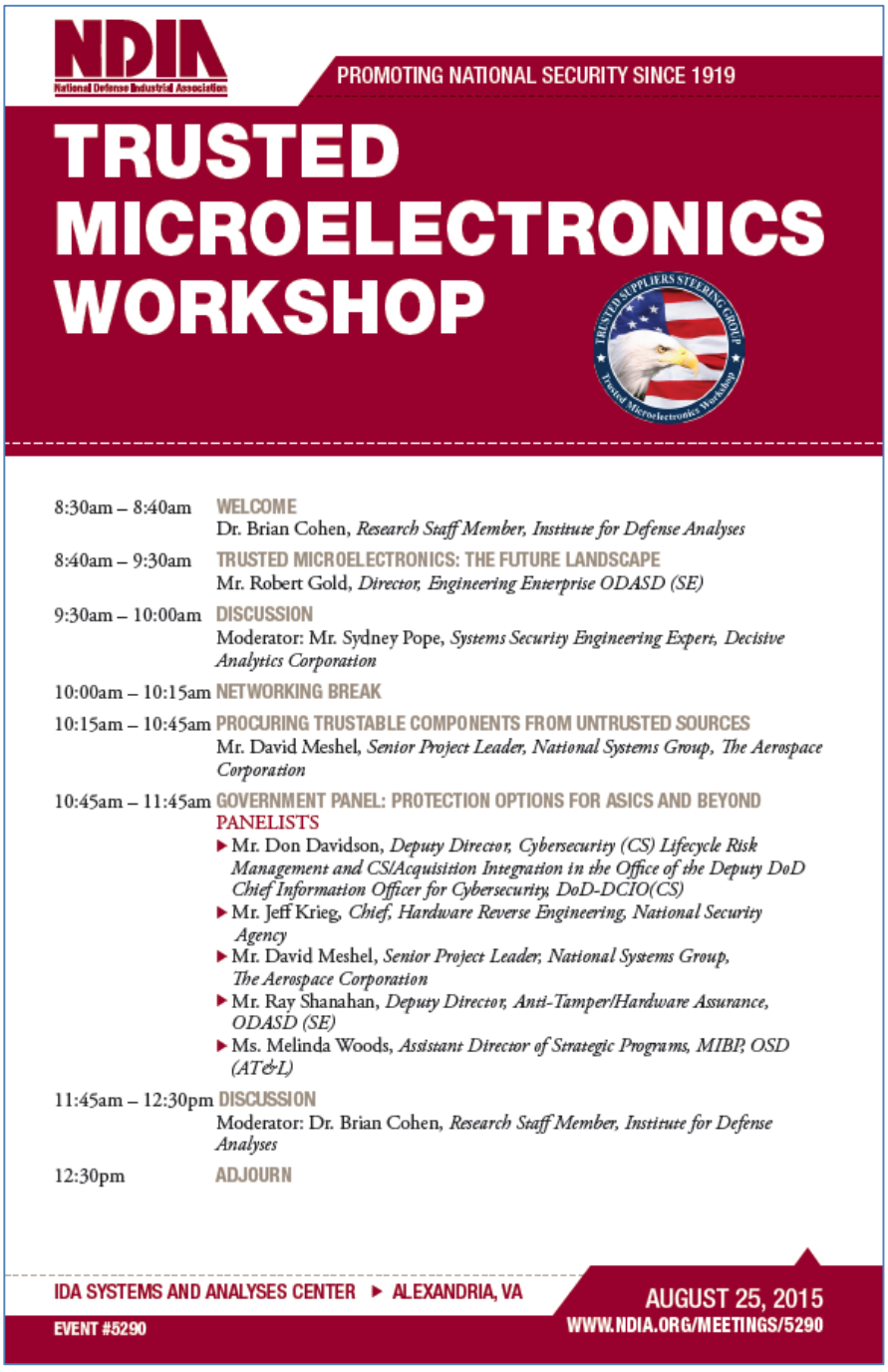
This fifth workshop in an ongoing series of workshops on Trusted Microelectronics was well attended and had excellent participation from the audience. The keynote by Mr. Robert Gold clearly conveyed the importance that DoD places on these issues. Mr. Gold communicated how there are a number of concerns ranging from malicious exploitation in the supply chain to counterfeit parts and the defects that occur in hardware products. His description of how these issues overlap between anti-tamper, policy, acquisition, providers, assured access and research highlights how complex the response to these issues has to be. He described a number of ongoing activities and introduced the audience to the JFAC.

Mr. David Meshel presented the approach being used by the space community that involves very specific supply chain control measures and extensive parts management. He noted that the space community has been very successful in virtually eliminating the occurrence of counterfeit parts in their applications. He also highlighted some of the policies and guidance that has been developed.

The panel discussions and open discussion was interesting and raised a range of concerns about the way forward. There are many differences in view about how to deal with protecting products that come from global commercial markets. It also isn't clear how government policies and practices can translate into industry and whether they will be at all relevant to the commercial suppliers. There was further discussion about how the security concerns of a broader community that includes commercial spaces and other nations might be mutually and collaboratively addressed.

In wrapping up the workshop, there was a discussion of the future direction of the Trusted Microelectronics Workshops. Many of the participants felt that a full day would be a more effective format. There was also a desire to include OEMs, integrators, security experts and contracting experts into the discussion.

Appendix A:
Agenda



Appendix B: Trusted Microelectronics: The Future Landscape, Robert Gold

B-2

Trusted Microelectronics: The Future Landscape

Robert Gold

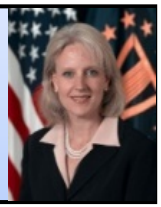
Director, Engineering Enterprise
ODASD, Systems Engineering

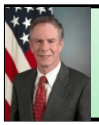
Assistant Secretary of Defense for Research and Engineering

NDIA Trusted Microelectronics Workshop, August 25, 2015

DASD, Systems Engineering

DASD, Systems Engineering
Stephen Welby
Principal Deputy Kristen Baldwin





Major Program Support
James Thompson

Supporting USD(AT&L) Decisions with Independent Engineering Expertise

- **Engineering Assessment / Mentoring of Major Defense Programs**
- **Program Support Assessments**
- **Overarching Integrated Product Team and Defense Acquisition Board Support**
- **Systems Engineering Plans**
- **Systemic Root Cause Analysis**
- **Development Planning/Early SE**
- **Program Protection**

Engineering Enterprise
Robert Gold

Leading Systems Engineering Practice in DoD and Industry

- **Systems Engineering Policy and Guidance**
- **Technical Workforce Development**
- **Specialty Engineering (System Safety, Reliability and Maintainability, Quality, Manufacturing, Producibility, Human Systems Integration)**
- **Security, Anti-Tamper, Counterfeit Prevention**
- **Standardization**
- **Engineering Tools and Environments**

Providing technical support and systems engineering leadership and oversight to USD(AT&L) in support of planned and ongoing acquisition programs

Engineering Enterprise Organization

Engineering Enterprise
Robert Gold

Systems Engineering Policy, Guidance, and Workforce
Aileen Sedmak

Engineering Tools and Environments: Digital Engineering Design, Engineered Resilient Systems, MOSA
Philomena Zimmerman

Specialty Engineering: R&M, Manufacturing, Value Engineering, System Safety
Andrew Monje

Software Assurance, Joint Federated Assurance Center (JFAC)
Thomas Hurt

Hardware Assurance, Anti-Tamper
Raymond Shanahan

System of Systems
Dr. Judith Dahmann

Standards & Standardization (DSPO)
Greg Saunders, Director
Stephen Lowell, Deputy

NATO/International/Web
Latasha Beckman
Procedures & DIDs
Karen Bond
DAU Liaison/Stdzn Journal/ PA/ASSIST/QPL/WSIT
Timothy Koczanski
Parts Mgmt/Qual Pgm
Donna McMurray
DMSMS/Counterfeit
Alex Melnikow
GIDEP/Anti-Counterfeit
James Stein
Budget Mgr, JSB
Lloyd Thomas
Non-Govt Stds/FARpt11
Trudie Williams

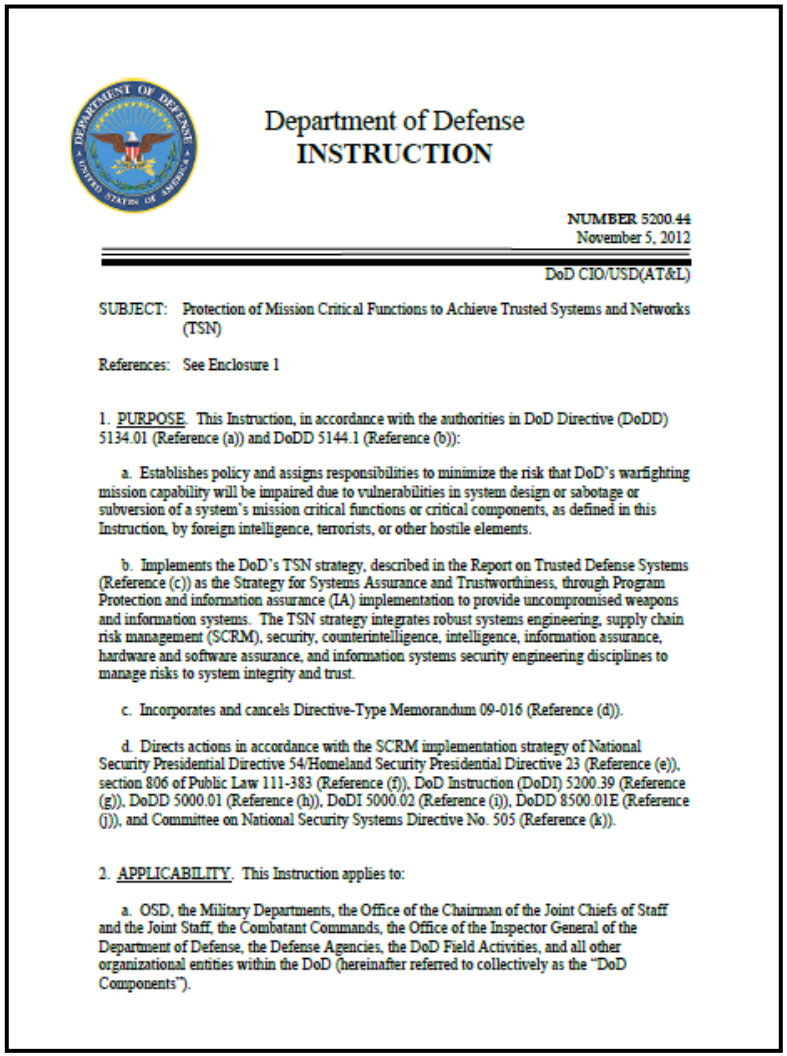
B-4

Engineering Enterprise Strategic Objectives

- **Manage the whole of our engineering activities**
  - Workforce
  - Tools and environments
  - Systems, domain-specific, and specialty engineering
  - Systems-of-systems
  - Assurance
  - Effectiveness
- **Establish collaboration with technical leads at major engineering activities and industry partners**
  - Foster information exchange
  - Identify and understand common challenges
  - Provide top cover for DoD Component and industry initiatives
  - Facilitate improvements to the state of practice, e.g., federating software assurance (SwA) and hardware assurance (HwA) people and organizations under Joint Federated Assurance Center (JFAC)
- **Promote investments in engineering S&T. For example:**
  - Automated detection of vulnerabilities and defects in the Department's software
  - Detection of binary malicious insertions in operational software
  - Innovative technologies for rapid inspection and analysis of microelectronics

Understand and Improve DoD's Collective Engineering Enterprise

Trusted Systems and Networks DoD Instruction 5200.44



Department of Defense
INSTRUCTION

NUMBER 5200.44
November 5, 2012

DoD CIO/USD(AT&L)

SUBJECT: Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)

References: See Enclosure 1

1. PURPOSE. This Instruction, in accordance with the authorities in DoD Directive (DoDD) 5134.01 (Reference (a)) and DoDD 5144.1 (Reference (b)):

a. Establishes policy and assigns responsibilities to minimize the risk that DoD's warfighting mission capability will be impaired due to vulnerabilities in system design or sabotage or subversion of a system's mission critical functions or critical components, as defined in this Instruction, by foreign intelligence, terrorists, or other hostile elements.

b. Implements the DoD's TSN strategy, described in the Report on Trusted Defense Systems (Reference (c)) as the Strategy for Systems Assurance and Trustworthiness, through Program Protection and information assurance (IA) implementation to provide uncompromised weapons and information systems. The TSN strategy integrates robust systems engineering, supply chain risk management (SCRM), security, counterintelligence, intelligence, information assurance, hardware and software assurance, and information systems security engineering disciplines to manage risks to system integrity and trust.

c. Incorporates and cancels Directive-Type Memorandum 09-016 (Reference (d)).

d. Directs actions in accordance with the SCRM implementation strategy of National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (Reference (e)), section 806 of Public Law 111-383 (Reference (f)), DoD Instruction (DoDI) 5200.39 (Reference (g)), DoDD 5000.01 (Reference (h)), DoDI 5000.02 (Reference (i)), DoDD 8500.01E (Reference (j)), and Committee on National Security Systems Directive No. 505 (Reference (k)).

2. APPLICABILITY. This Instruction applies to:

a. OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (hereinafter referred to collectively as the "DoD Components").

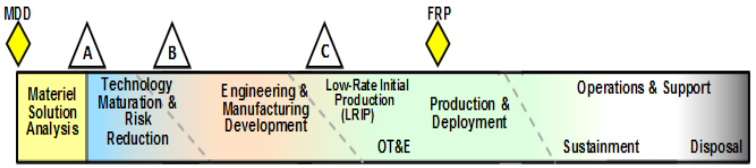
- **Implements the DoD's Trusted Systems and Networks (TSN) strategy**
- **Manage risk of mission-critical function and component compromise throughout lifecycle of key systems by utilizing**
  - Criticality Analysis as the systems engineering process for risk identification
  - Countermeasures: Supply chain risk management, software assurance, secure design patterns
  - Intelligence analysis to inform program management
- **Codify trusted supplier requirement for DoD-unique application-specific integrated circuits (ASICs)**
- **Document planning and accomplishments in program protection and information assurance activities**

B-6

Malicious Supply Chain Risk

- ***Threat:***
  - Nation-state, terrorist, criminal, or rogue developer who gains control of ***systems or information*** through supply chain opportunities; exploits vulnerabilities remotely, and/or degrades system behavior
- ***Vulnerabilities:***
  - All systems, networks, and applications
  - Intentionally implanted logic (HW/SW)
  - Unintentional vulnerabilities maliciously exploited (e.g., poor quality or fragile code)
  - Controlled unclassified information resident on, or transiting supply chain networks
- ***Consequences:***
  - Loss of data; system corruption
  - Loss of confidence in critical warfighting capability; mission impact

Access points are throughout the acquisition lifecycle…

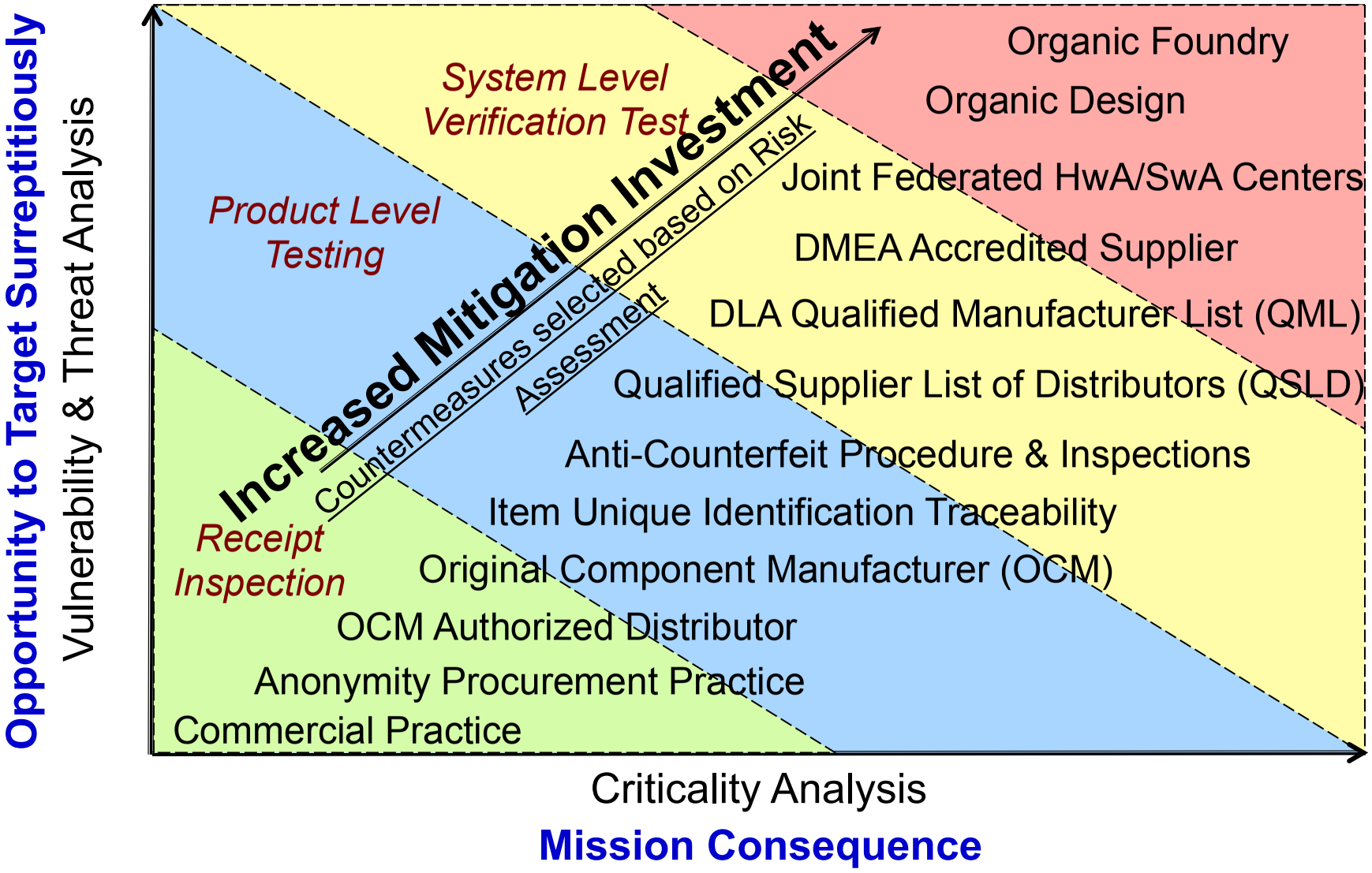


…and across numerous supply chain entry points

- Government
- Prime, subcontractors
- Vendors, commercial parts manufacturers
- 3rd party test/certification activities

B-7

Supply Chain Risk Countermeasures



Software and Hardware Assurance (SwA/HwA) Summary of Objectives

- **Strategic Planning**
  - Facilitate and incorporate activities which establish HwA and SwA as disciplines of SE
  - Participate in forums which help to grow, provide visibility, and establish relationships for the DoD HwA and SwA communities
- **Policy and Guidance Development**
  - Integrate Congressional legislation (NDAA 932, 933, 937) into DoD acquisition policy and guidance
  - Develop community white papers that provide specific focused guidance
  - Integrate DT, OT&E and L&MR functions into HwA and SwA guidance and procedures
- **Support to Program Protection Planning (PPP)**
  - Develop and provide resource materials that mentor, coach, and teach integration of HwA and SwA in program acquisition strategies
  - Provide consistency in policy and guidance documents relevant to developing HwA and SwA strategies in PPPs (DAG, PPP Outline and Guidance, PPP Evaluation Criteria, DoDI 5000.02, and industry best practices)
- **Outreach**
  - Mature the SwA Community of Practice and develop a HwA Community of Practice leveraging existing forums
  - Support HwA and SwA community outreach through collaboration tools (SharePoint, Defense Collaboration Services and voice conferencing)
  - Develop and support HwA and SwA workforce training

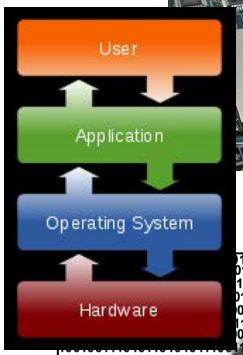
Hardware Assurance

Control the quality, configuration, and security of software, firmware, hardware, and systems throughout their lifecycles, including components or subcomponents from secondary sources. Employ protections that manage risk in the supply chain for components or subcomponent products and services (e.g., ICs, FPGA, printed circuit boards) when they are identifiable (to the supplier) as having a DoD end-use. – DoDI 5200.44

B-10

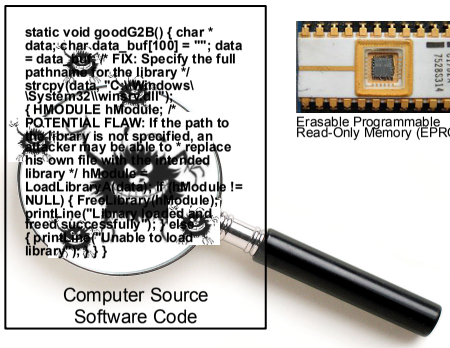
- **Program Protection Plan (PPP) identifies system's Critical Functions and Critical Components w/focus on Integrated Circuits (ICs)**
  - Custom Application Specific Integrated Circuits, Field Programmable Gate Arrays, etc. are identified for protection from malicious attacks
- **PPP addresses how protections are implemented at each program milestone phase:**
  - Component testing, including logic, imaging, signal and thermal testing, and system-level testing
  - Process controls, including anti-counterfeit and supply "chain of custody"

Joint Federated Assurance Center (JFAC)



Field Programmable Gate Array

Binary Computer Software Code



Computer Source Software Code

Erasable Programmable Read-Only Memory (EPROM)

B-11

Assure Mission SW and HW Security

Intent:

- Congress directed DoD to "…*provide for the establishment of a joint federation of capabilities to support the trusted defense system needs…to ensure security in the software and hardware developed, acquired, maintained, and used by the Department.*" (FY14 NDAA, Sect. 937)

Expected Outcomes/Deliverables:

- Federated cross-DoD awareness and coordination of software and hardware assurance (SwA/HwA) capabilities and expertise
- Development and sharing of SwA/HwA vulnerability assessment best practices, tested tools, and proven processes
- Identification of R&D needs to advance SwA/HwA capabilities for programs in acquisition, operational systems, and legacy systems and infrastructure

Key Participants:

- Sponsor(s): ASD(R&E)/DASD(SE)
- Contributors: CIO, AF, Army, Navy, USMC, NSA, NRO, MDA, DISA, Defense Microelectronics Activity (DMEA)

Approach:

- Establish federation of HwA and SwA capabilities to support programs in program protection planning and execution
- Support program offices across life cycle by identifying and facilitating access to Department SwA and HwA expertise and capabilities, policies, guidance, requirements, best practices, contracting language, training, and testing support
- Coordinate with DoD R&D for HwA and SwA
- Procure, manage, and distribute enterprise licenses for SwA/HwA tools

Milestones:

Formed Steering Committee and Working Groups	7/14
Initiated First Series of Technical Tasks	9/14
Charter signed by Deputy Secretary of Defense	2/15
Congressional Report on funding, organization, management, and operations of JFAC signed & submitted	3/15
CONOPS signed by stakeholders of Federation	8/15
Capability Assessment, Gap Analysis, Strategic Plan	10/15
Joint Federated Assurance Center (JFAC) IOC	12/15

Counterfeit Prevention and Diminishing Sources

- **Develop and implement a risk-based approach to identify critical materiel**
- **Develop and modify quality assurance policy, procedures and standards**
- **Incorporate design considerations in the Defense Acquisition Guidebook (DAG)**
- **Establish technical qualification criteria for suppliers (trustworthy)**
- **Implement enhancements to Government and Industry Data Exchange Program (GIDEP) to expand its usefulness and robustness in the DoD global supply chain**
- **Research and develop support tools and techniques**
- **Execute Diminishing Manufacturing Sources and Material Shortages (DMSMS) program strategy**
  - Reduce or eliminate the cost and schedule impacts of identified DMSMS issues
  - Ensure that DMSMS issues do not prevent weapon system readiness and performance goals from being met

The Advanced Semiconductor Quandary

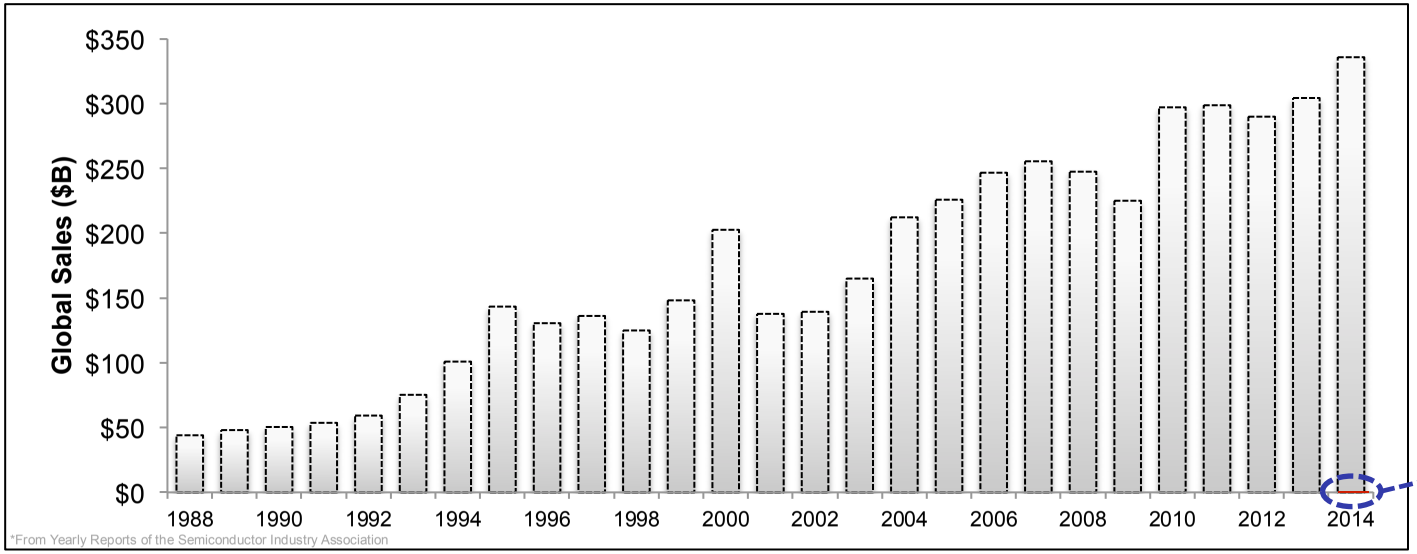
Foundry choices
Commercial: Multiple global options
DoD: One

Order size
Commercial: 100Ks to Ms
DoD: 100s to Ks

Chip Prototype-to-System Production
Commercial: 9-10 months
DoD: 4-10 years

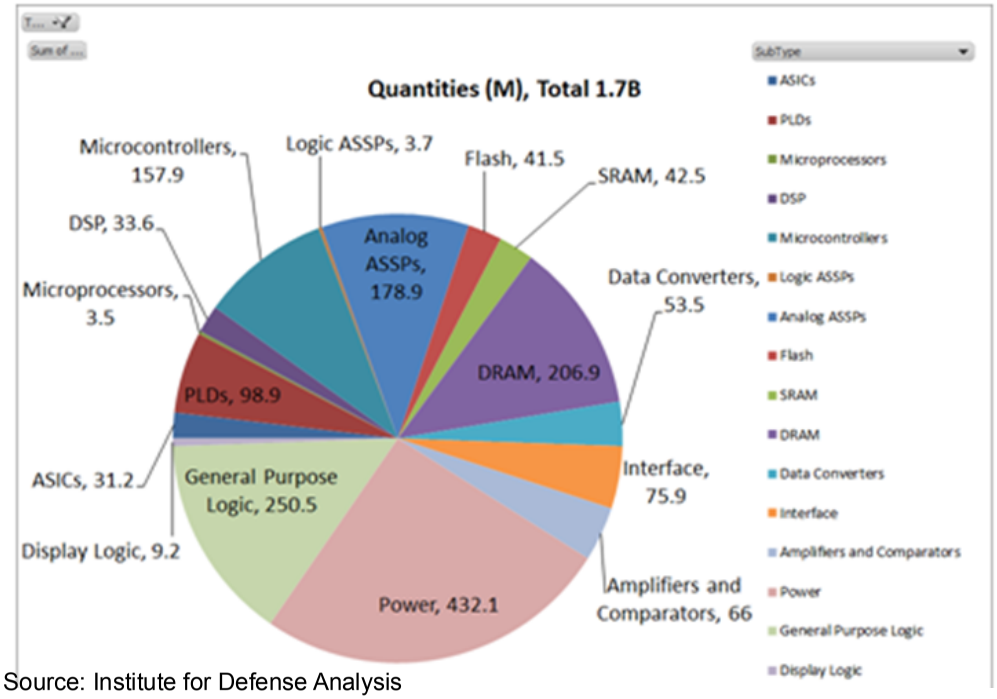
DoD is an insignificant portion of the > $300B global electronics market at <$1B.

The commercial sector drives the market!



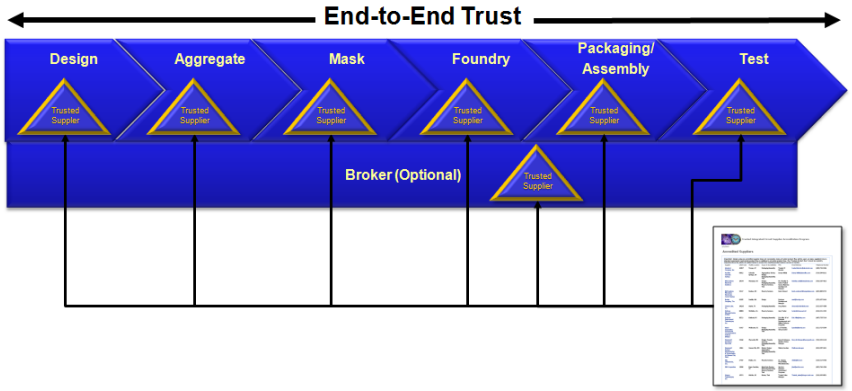
Trusted Microelectronics

- **Application Specific Integrated Circuit (ASIC) policy: DoD custom end use ASICs can only be procured from a DMEA-accredited Trusted Supplier**
  - Accounts for <2% of the 1.9B ICs DoD acquires per year
  - In general order of interest for trust: ASICs, FPGAs, Microprocessors, Logic Application Specific Standard Products, Memories, A-D Converters, Interface Chips
- **What is needed:**
  - A risk-based process for identification and prioritization of all critical ICs to address risk mitigation across life-cycle
  - More effective and affordable risk mitigation countermeasures for ICs
  - Continued collaboration between government, industry, and academia



Source: Institute for Defense Analysis

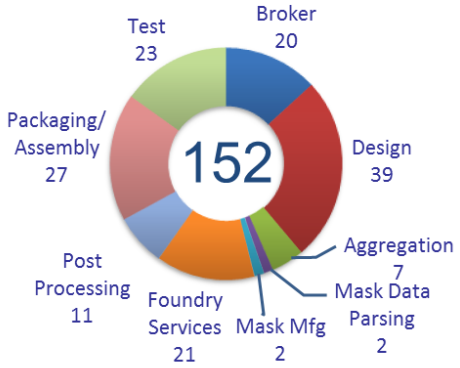
Trusted Foundry Program



- **Only method to obtain quick-turn, Trusted microelectronics (protecting integrity, confidentiality and availability)**
  - Mitigates risk of hardware Trojan insertion per DoDI 5200.44
  - Protects Critical Program Information per DoDI 5200.39
- **Major elements**
  - Long term contract to secure Trusted access to leading-edge foundry technology
  - Accreditation of Trusted Suppliers across the entire supply chain
- **Trusted Suppliers must meet a comprehensive set of security and quality criteria**
  - Facility Clearance, FOCI adjudication/mitigation
  - Cleared Chain of Custody
  - Information System Security
  - Configuration Management
  - Quality
  - Manufacturing Contingency Plan
  - Scrap Controls
- **Equally funded by NSA and DMEA**

- **Cost: Trusted services ~18% more than non-ITAR services**
- **Schedule impact: zero to less than zero (some suppliers give priority to Trusted services)**
- **Caveat: Trusted services must be explicitly requested from a designated POC at the Trusted supplier**

Total Accredited Services



As of 5 Aug 2015

B-15

A DoD System

Bill of Material (BOM) excerpt from Program Protection Plan (PPP) review

LV	Part Number	Nomenclature	QPA	Unit Price	Material
03	602358-029	ABC SUB/ASSY	1	$0.00	0.0001
03	0089-1A33	HUMISEAL,TY UR,CL B,GAL	0.01	$0.00	0
03	MC-0402-875	POLYURETHAN ADH,875 GM KT	0.01	$0.00	0
03	25ACL71-M	MAG., MODULE, P/S	1	$0.00	0.0001
03	030C-M	DC-DC	1	$0.00	0.0001
03	C075F1	MAG., MODULE, P/S	1	$0.00	0.0001
03	S3755/1-10	POWDER,FUME SILI 10LB BAG	0.0001	$0.00	0
04	548FKTWREP	MICROCIRCUIT (REELED)	12	$15.01	180.1572
04	413ES	MICROCIRCUIT (REELED)	11	$9.69	106.5559
05	003A0A94	PWR SUPPLY DC-DC	1	$0.00	0.0001
05	015C91	P/S MODULE,DC-DC	2	$0.00	0.0002
05	XYZ-1553GT	MICROCIRCUIT (REELED)	1	$428.91	428.9061
05	2V500-4FG456I	MCKT (MATRIX TRAYED)	1	$199.52	199.5246
05	602458-001	ABC PWB	1	$233.12	233.1221

Part number	**XYZ-1553GT**
Category	**Communication => Others**
Description	Description = **MIL-STD-1553, Dual Redundant, Remote Terminal, 4k Words Static RAM, Multichip, Monolithic Transceivers REDACTED VERSION**

A DoD System

Bill of Material (BOM) excerpt from Program Protection Plan (PPP) review

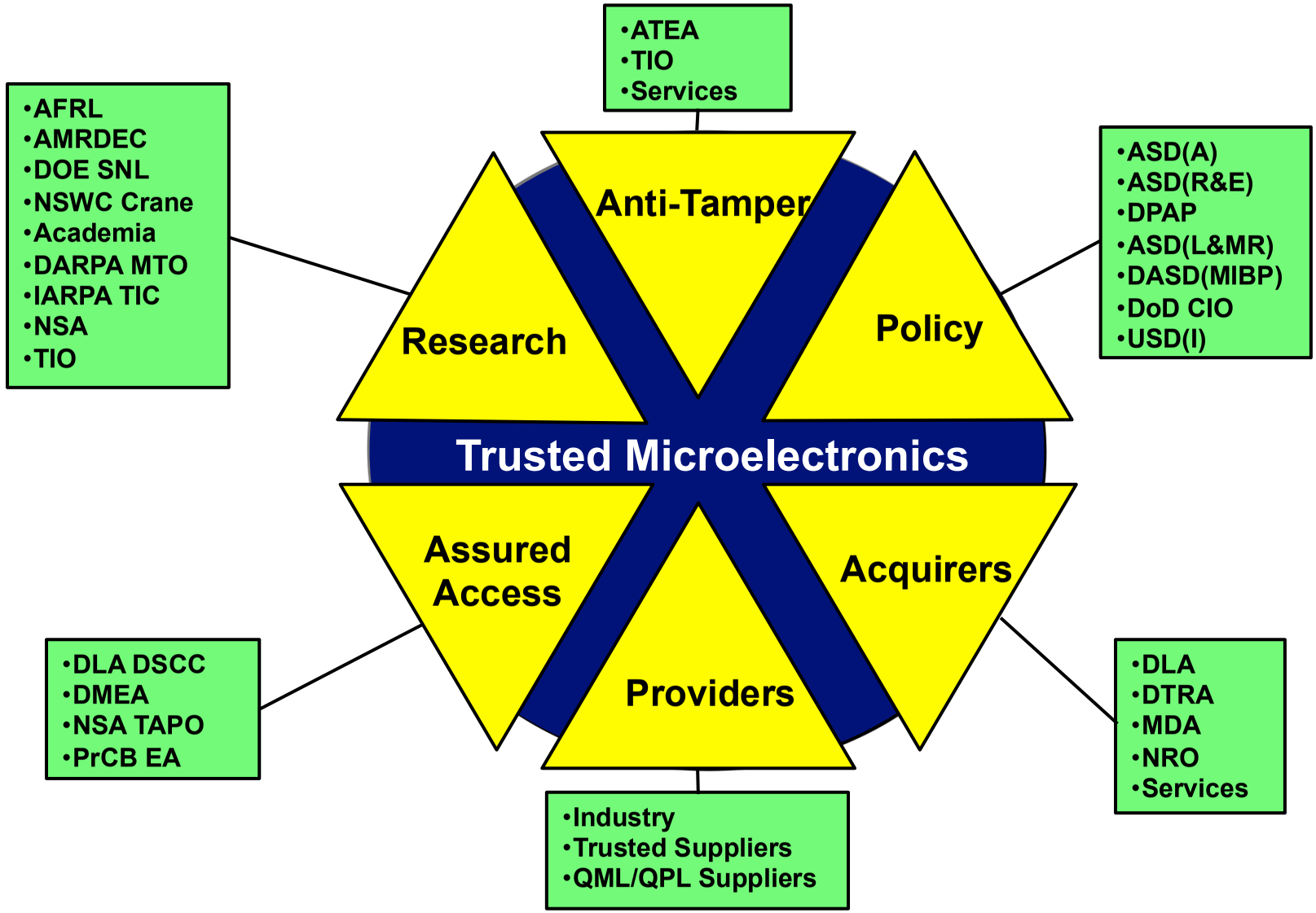
LV	Part Number	Nomenclature	QPA	Unit Price	Material
03	602358-029	ABC SUB/ASSY	1	$0.00	0.0001
03	0089-1A33	HUMISEAL,TY UR,CL B,GAL	0.01	$0.00	0
03	MC-0402-875	POLYURETHAN ADH,875 GM KT	0.01	$0.00	0
03	25ACL71-M	MAG., MODULE, P/S	1	$0.00	0.0001
03	030C-M	DC-DC	1	$0.00	0.0001
03	C075F1	MAG., MODULE, P/S	1	$0.00	0.0001
03	S3755/1-10	POWDER,FUME SILI 10LB BAG	0.0001	$0.00	0
04	548FKTWREP	MICROCIRCUIT (REELED)	12	$15.01	180.1572
04	413ES	MICROCIRCUIT (REELED)	11	$9.69	106.5559
05	003A0A94	PWR SUPPLY DC-DC	1	$0.00	0.0001
05	015C91	P/S MODULE,DC-DC	2	$0.00	0.0002
05	XYZ-1553GT	MICROCIRCUIT (REELED)	1	$428.91	428.9061
05	2V500-4FG456	MCKT (MATRIX TRAYED)		$199.52	199.5246
05	602458	ABC PWB			

A commercial hybrid circuit designed for use with military avionics, but also commonly used in aerospace systems; in this case, provides a communications interface between the weapon and the mission computer

Made in U.S., but sold world-wide; available for purchase from independent brokers

B-17

Major Participating Organizations



Future Challenges

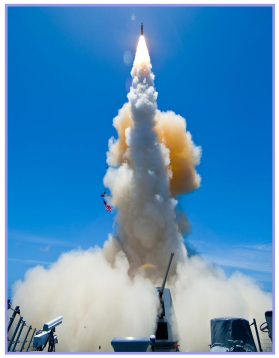
- **Making cost effective decisions for programs to deal with changing commercial foundry capabilities – assured access**
  - End of life buy
  - Subsidize commercial
  - Migrate to current or emerging production technology
  - Purchase foundry equipment for organic production
  - Emerging business models for low volume foundries
- **Ensuring we can trust our parts or trust our assemblies of untrusted parts**
  - New approaches to chip design
  - New approaches to V&V
  - New approaches to circuit and system design
- **Dealing with the increasingly 'software-like' behavior of the hardware community**
  - Rapid migration of technology
  - Decreasing influence of DoD on technical and business foundations
  - Design flexibility and ease of field update
  - Increasing ease of tampering, counterfeits, and reverse engineering

The Way Ahead

- **Program engagement**
  - Foster early planning for HwA and SwA, design with security in mind
  - Implement expectations in plans and on contract
  - Support vulnerability analysis and mitigation needs
- **Community collaboration**
  - Achieve a networked capability to support DoD needs: shared practices, knowledgeable experts, and facilities to address malicious supply chain risk
- **Industry engagement**
  - Communicate strategy to tool developers
  - Develop standards for common articulation of vulnerabilities and weaknesses, capabilities and countermeasures
- **Advocate for R&D**
  - HwA and SwA tools and practices
  - Strategy for trusted microelectronics that evolves with the commercial sector
- **People!**
  - Improve awareness, expertise to design and deliver trusted systems

Systems Engineering: Critical to Defense Acquisition










B-21

Defense Innovation Marketplace
http://www.defenseinnovationmarketplace.mil

DASD, Systems Engineering
http://www.acq.osd.mil/se

Acronyms

AFRL	Air Force Research Laboratory
AMRDEC	U.S. Army Aviation and Missile Research, Development and Engineering Center
ATEA	Anti-Tamper Executive Agent
DARPA MTO	Defense Advanced Research Projects Agency Microelectronics Technology Office
DLA DSCC	Defense Logistics Agency, Defense Supply Center, Columbus
DOE SNL	Department of Energy Sandia National Laboratory
IARPA TIC	Intelligence Advanced Research Projects Activity Trusted Integrated Chips
NSA TAPO	National Security Agency Trusted Access Project Office
NSWC Crane	Naval Surface Warfare Center Crane
PrCB EA	Printed Circuit Board Executive Agent
QML	Qualified Manufacturer List
QPL	Qualified Products List
TIO	Technology Integration Office

Additional Information

DASD(SE)/EE, Systems Engineering Policy and Guidance

Policy

- **New DoD Instruction 5000.02 released January 7, 2015 (supersedes & replaces the interim version issued on November 25, 2013)**
  - Modifications made to Enclosure 3, Systems Engineering, but no new requirements were added

DoDI 5000.02 (7 Jan 2015)
Enclosure 3 Systems Engineering

1. Purpose
2. Systems Engineering Plan
3. Development Planning
4. Systems Engineering Trade-Off Analyses
5. Technical Risk and Opportunity Management
6. Technical Performance Measures and Metrics
7. Technical Reviews
8. Configuration Management
9. Modeling and Simulation
10. Manufacturing and Producibility
11. Software
12. Reliability and Maintainability
13. Program Protection
14. Open Systems Architectures
15. Corrosion Prevention and Control
16. Environment, Safety, and Occupational Health
17. Insensitive Munitions
18. Item Unique Identification
19. Spectrum Supportability
20. ~~Design Reviews~~
21. Program Support Assessments

merged content

Blue = Sections that contain revisions

B-24

DASD(SE)/EE, Systems Engineering Policy and Guidance

- **Guidance**
  - Department of Defense Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs (DoD RIO Guide) published June 2015
    - Supports the Better Buying Power 3.0 initiative: Improve our leaders' ability to understand and mitigate technical risk
    - Ensures understanding, implementation, and reporting of risk identification, management, and mitigation across the Department
- **Standards Development**
  - IEEE 15288.1-2014, "IEEE Standard for Application of Systems Engineering on Defense Programs"
  - IEEE 15288.2-2014, "IEEE Standard for Technical Reviews and Audits on Defense Programs"
  - SAE AS6500, "Manufacturing Management Program"
  - EIA 649_1, "Configuration Management Requirements for Defense Contracts"

B-25

Defense Standardization

- **Defense Standardization Council identified key initial areas where standards are needed to restore discipline and consistency**
  - Systems engineering
  - Technical reviews and audits
  - Configuration management
  - Manufacturing management
  - Logistics support analysis
- **Focus is on supporting Department needs by leveraging voluntary consensus standards**
- **Future focus: Identifying key areas where additional standards can drive acquisition effectiveness and efficiency**
  - Modular Open Systems Architecture
  - Human systems integration
  - Corrosion control and prevention

Specialty Engineering Summary of Objectives

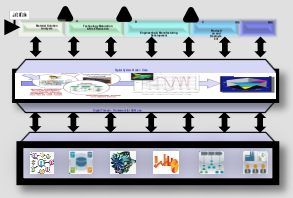
- **Reliability and Maintainability Engineering**
  - Continue Program Engagement
  - Continuous Improvement of Policy and Guidance
  - Enhance DoD and Industry Outreach
  - Enhance R&M Engineering Workforce
- **Manufacturing Engineering**
  - Expand Program Engagement
  - Refine Body of Knowledge
  - Maintain Vigorous Outreach
- **Human Systems Integration (HSI)**
  - SE Focal Point (Joint HSI Steering Committee, HSI Standards Working Group)
- **Value Engineering (VE)**
  - Support DoDI 4245.14 Requirements
  - Foster and Recognize VE Achievement

Engineering Tools and Environments

Engineering Tools and Environments

Digital Engineering Design

- Digital System Model/ Digital Thread
- Education
- Policy & Guidance
- Data Rights

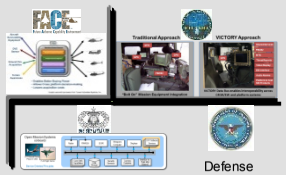


Engineered Resilient Systems

- Trade Space Analysis
- SERC
- CREATE/HPCMO

Modular Open Systems Architecture

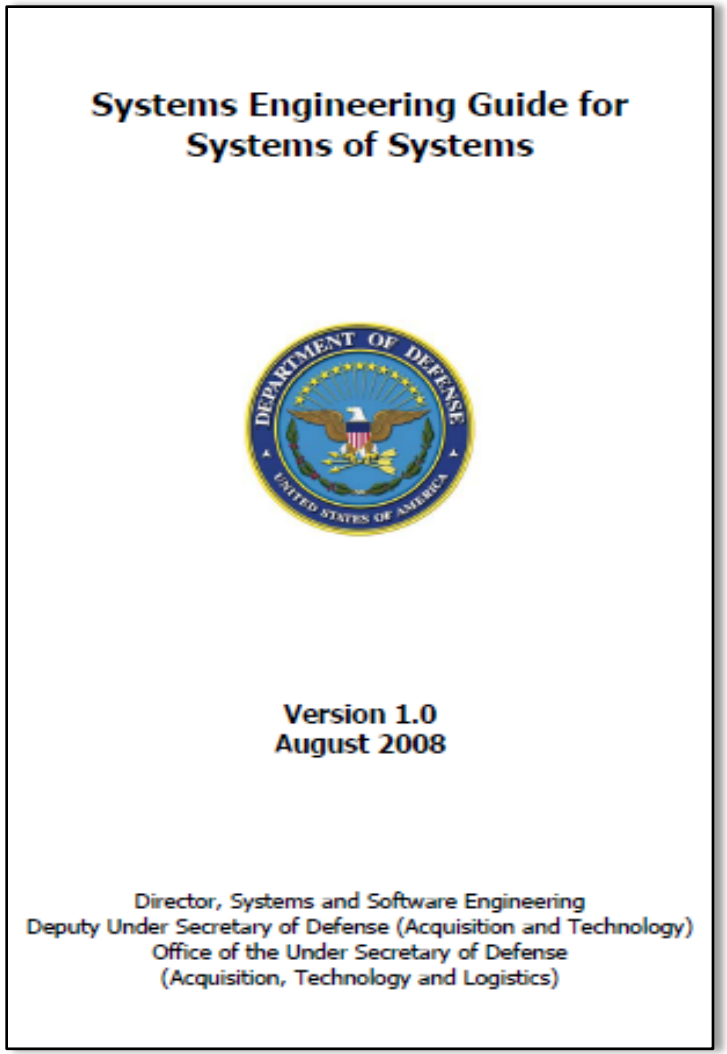
- BBP 3.0
- Technical Standards
- SERC



Outreach: AMSWG, NDIA, MBE Summit, INCOSE/JPL

Engineering processes, specialty engineering methods and tools to incorporate the latest digital practices for making informed decisions throughout the acquisition lifecycle.

Systems of Systems Engineering Summary of Objectives



- **Refresh current body of practice based on the last 4-5 years of DoD experiences**
- **Identify 1-3 joint warfighting areas to apply improved practice and lessons learned**

Appendix C:
Procuring Trustable Components From Untrusted Sources, David Meshel

David Meshel's presentation can be requested
by contacting him at:
david.c.meshel@aero.org

Appendix D:
Attendees

John Robert Adams, The Aerospace Corporation

Luis Ancajas, Intrinsic ID

Brett Attaway, Synopsys, Inc.

Peter Behrens, National Security Agency

Tom Bergman, Battelle

Peter C. Broadbent, Photronics, Inc.

Theodore Bujewski, DASD(MIBP)

Patrick Cheetham, Potomac Institute for Policy Studies

Brian Cohen, Institute for Defense Analyses

Lew Cohn, National Reconnaissance Office

Douglas Cummings, The Aerospace Corporation

Chris Daverse, Defined Business Solutions

Donald R. Davidson, Jr., Office of the Deputy CIO for CyberSecurity (CS), DoD CIO

Paul de Naray, The Aerospace Corporation

Wayne A. DeCarlo, Photronics, Inc.

Glen Duke, National Security Agency

Gerald Wayne Etzold, Etzold Technology Consulting

Bradley Alan Ferguson, Cypress Semiconductor Corporation

Michael Fritze, Potomac Institute for Policy Studies

Jim Gobes, Intrinsix

Robert Gold, OSD, AT&L

Jason Gorey, Defined Business Solutions

Brian Hagerty, Hagerty Consulting

Rebecca Horton,

Selim S. Ibrahim, Office of the Secretary of Defense

Walter W. Jaron, Northrop Grumman

Michael H Johnson, Sandia National Laboratories

Scott L. Jordan, Jazz Semiconductor Trusted Foundry

Stylianos Kaminaris, Battelle

Nicholas S.J. Karvonides, Institute for Defense Analyses

Harry G. Kellzi, Teledyne Microelectronic Technologies

Gary T Kiefer, Rockwell Collins

Kathleen N. Kingscott, IBM Corporation

Elizabeth Janet Klein-Lebbink, The Aerospace Corporation

Jeff Krieg, National Security Agency

Jennifer Lato, Potomac Institute for Policy Studies

Kenneth Lebo, Van Dyke Technology Group

Kathy Lee, Institute for Defense Analyses

Jeff Magee, GLOBALFOUNDRIES

Mark E Marson, Cryptography Research, Inc.

Mona Massuda, Department of Defense

Greg McCarthy, ON Semiconductor

Michael F. McGrath, McGrath Analytics, LLC

Michael J. Mehlberg, Cryptography Research, Inc.

David Meshel, The Aerospace Corporation

Robert S. Metzger, Rogers Joseph O'Donnell, PC

Jeffrey A. Miller, Northrop Grumman Electronic Systems

Joseph Misanin, Misanin Technology Ventures, LLC.

John Lawrence Monk, Jr., Northrop Grumman

Michael Russell Moore, Cypress Semiconductor Corporation

Robert Moriarty, EndoSec

Jonah Nelson,

Terita Norton, The Aerospace Corporation

Stewart L Ocheltree, BAE Systems

Catherine J. Ortiz, Defined Business Solutions

Doug Palmer, Booz Allen Hamilton

Gregg Panning, Honeywell Corp

Sydney Pope, Decisive Analytics Corporation

Jimmy Poplin, Defined Business Solutions

Andrew Popp, Aeroflex Incorporated

Paul Quirk, National Secure Manufacturing Center

Mark Redlinger, Equator Corp

Kirk Reynolds, Rockwell Collins

VJ Sahi, Clark Street Associates

Timothy Scott, Novati Technologies

Raymond C. Shanahan, DASD(SE)

Marko M. G. Slusarczuk, Institute for Defense Analyses

Perry A. Tapp, Kansas City Plant

Stephen Tetlak,

Samantha Ulrich, Northrop Grumman Electronic Systems

Kenneth Wetzel, Jr., Strategic Marketing Innovations

F. Peter Wheatley, DoD

Chuck White, Sypris Electronics LLC

Melinda Woods, DASD(MIBP)

Huan Zhang, Institute for Defense Analyses