



2014 Diminishing Manufacturing Sources and Material Shortages (DMSMS) Conference Keynote Address

Mr. Robert A. Gold

Director, Engineering Enterprise

**Office of the Deputy Assistant Secretary of Defense for Systems
Engineering (ODASD(SE))**

December 2, 2014



Outline



Source

Initiative

OSD Leadership

- **Better Buying Power 3.0**

Acquisition Req'ts

- **Program Protection Planning**

Community Activities



- **Counterfeit Parts**
- **Joint Federated Assurance Center (JFAC)**
- **Trusted Microelectronics**
- **Manufacturing**



Better Buying Power (BBP) 3.0



- Interim release made on September 19, 2014
- Continues a focus on continuous improvement with a new emphasis on encouraging innovation
- Includes all BBP 2.0 initiatives that were not completed
 - Some initiatives continued without specific emphasis
 - Some initiatives continued without change or with some modifications



Better Buying Power 3.0 DRAFT

Achieving Dominant Capabilities through Technical Excellence and Innovation

Achieve Affordable Programs

- Continue to set and enforce affordability caps

Achieve Dominant Capabilities While Controlling Lifecycle Costs

- Strengthen and expand "should cost" based cost management
- Build stronger partnerships between the acquisition, requirements, and intelligence communities
- Anticipate and plan for responsive and emerging threats
- Institutionalize stronger DoD level Long Range R&D Planning

Incentivize Productivity in Industry and Government

- Align profitability more tightly with Department goals
- Employ appropriate contract types, but increase the use of incentive type contracts
- Expand the superior supplier incentive program across DoD
- Increase effective use of Performance-Based Logistics
- Remove barriers to commercial technology utilization
- Improve the return on investment in DoD laboratories
- Increase the productivity of IRAD and CR&D

Incentivize Innovation in Industry and Government

- Increase the use of prototyping and experimentation
- Emphasize technology insertion and refresh in program planning
- Use Modular Open Systems Architecture to stimulate innovation
- Increase the return on Small Business Innovation Research (SBIR)
- Provide draft technical requirements to industry early and involve industry in funded concept definition to support requirements definition
- Provide clear "best value" definitions so industry can propose and DoD can choose wisely

Eliminate Unproductive Processes and Bureaucracy

- Emphasize Acquisition Executive, Program Executive Officer and Program Manager responsibility, authority, and accountability
- Reduce cycle times while ensuring sound investments
- Streamline documentation requirements and staff reviews

Promote Effective Competition

- Create and maintain competitive environments
- Improve technology search and outreach in global markets

Improve Tradecraft in Acquisition of Services

- Increase small business participation, including more effective use of market research
- Strengthen contract management outside the normal acquisition chain
- Improve requirements definition
- Improve the effectiveness and productivity of contracted engineering and technical services

Improve the Professionalism of the Total Acquisition Workforce

- Establish higher standards for key leadership positions
- Establish stronger professional qualification requirements for all acquisition specialties
- Strengthen organic engineering capabilities
- Ensure the DOD leadership for development programs is technically qualified to manage R&D activities
- Improve our leaders' ability to understand and mitigate technical risk
- Increase DoD support for Science, Technology, Engineering and Mathematics (STEM) education

**Continue Strengthening Our Culture of:
Cost Consciousness, Professionalism, and Technical Excellence**



DMSMS Contributions to BBP 3.0



- **Achieve dominant capabilities while controlling lifecycle costs by...**
 - Attaining should cost targets based on DMSMS inputs to design
- **Incentivize productivity in industry and government by ...**
 - Cultivating long-term relationships with suppliers
- **Incentivize innovation in industry and government by ...**
 - Informing technology refresh and insertion planning with obsolescence projections
- **Promote effective competition by ...**
 - Using design principles that make it easier to find alternative parts and suppliers
- **Improve tradecraft in acquisition of services by ...**
 - Creating contract incentives to encourage industry to manage DMSMS issues
- **Improve the professionalism of the total acquisition workforce by...**
 - Identifying risk-based approaches for proactive DMSMS monitoring



Program Protection Planning



Protecting Acquisition Programs

Program Protection Planning

Interim DoDI 5000.02

DoDI 5200.39

DoDI 5200.44

DoDI 8500.01

Technology

Components

Information

What: Leading-edge research and technology

Who Identifies: Technologists, System Engineers

ID Process: CPI identification

Threat Assessment: Foreign collection threat informed by Intelligence and Counterintelligence (CI) assessments

Countermeasures: AT, classification, export controls, security, foreign disclosure, and CI activities

Focus: "Keep secret stuff in" by protecting any form of technology

What: Mission-critical elements and components

Who Identifies: System Engineers, Logisticians

ID Process: Criticality analysis

Threat Assessment: DIA SCRM TAC

Countermeasures: Hardware and software assurance, SCRM, anti-counterfeit, Trusted Foundry, Trusted Suppliers, etc.

Focus: "Keep malicious stuff out" by protecting key mission components

What: Information about applications, processes, capabilities and end-items

Who Identifies: All

ID Process: CPI identification, criticality analysis, and classification guidance

Threat Assessment: Foreign collection threat informed by Intelligence and CI assessments

Countermeasures: Cybersecurity, classification, export controls, security, etc.

Focus: "Keep critical information from getting out" by protecting data

Protecting Warfighting Capability Throughout the Lifecycle



Program Protection Integrated Supply Chain Policy

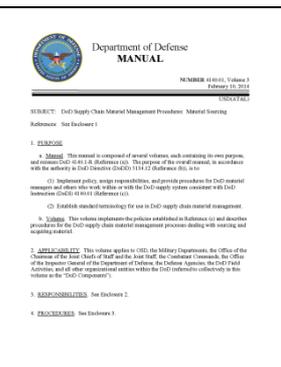
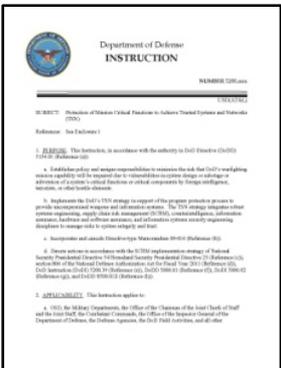
DoDI 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)

- Requires AT&L to develop a strategy for managing risk in the supply chain for integrated circuit-related products and services (e.g., FPGAs, printed circuit boards) that are identifiable to the supplier as specifically created or modified for DoD (e.g., military temperature range, radiation hardened).

DoDM 4140.01 DoD Supply Chain Materiel Management Procedures, Volume 3

- Requires quality assurance methods including contractor selection and qualification programs; quality requirements; pre-award surveys; Government inspection; and testing.
- Quality assurance techniques and testing should stress conforming Critical Application Item (CAI) to contract and technical requirements.

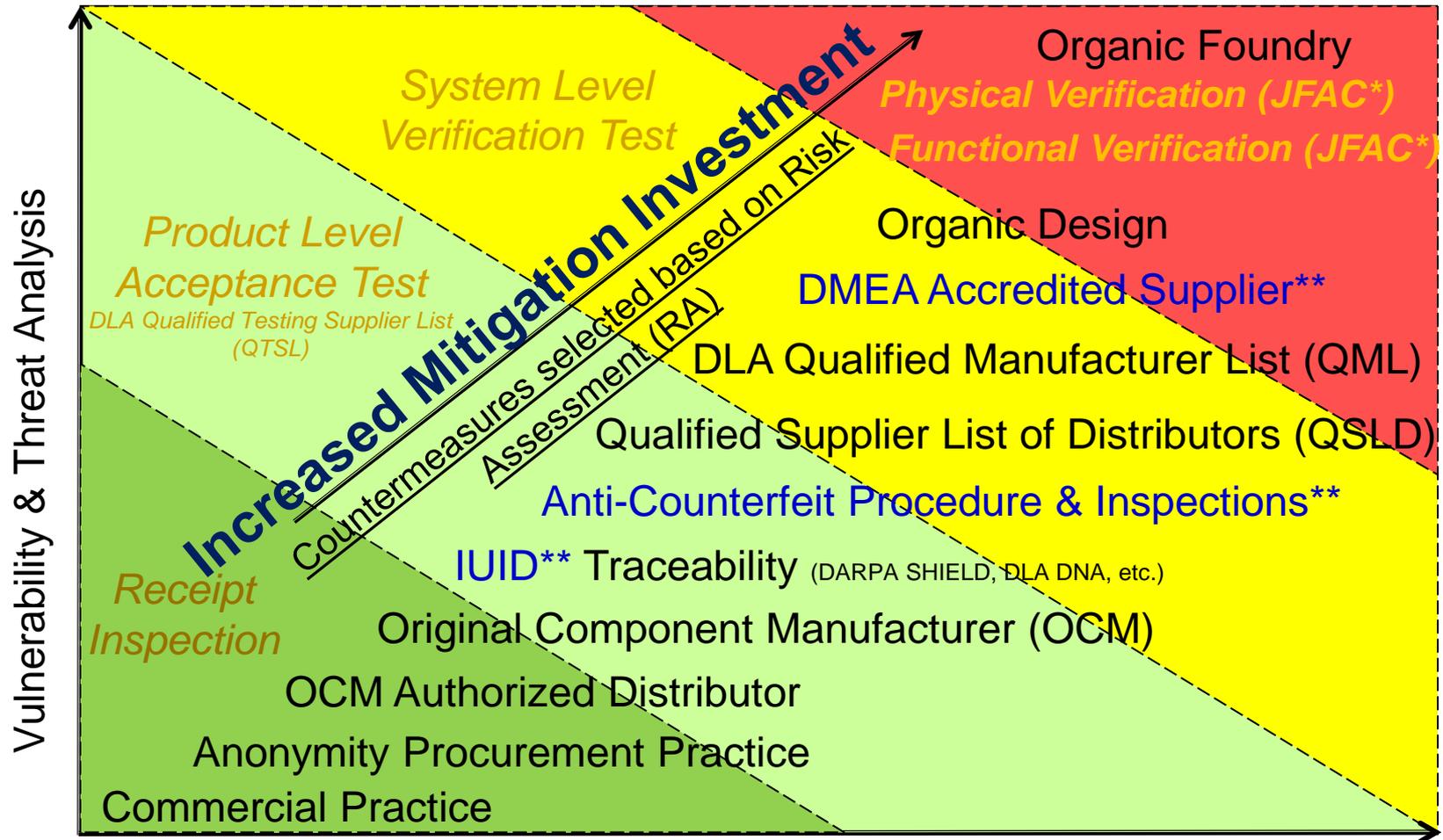
Security risk criteria should be added to safety, reliability, etc. for CAI designation in the supply chain to assist in managing microelectronics CCs throughout the acquisition lifecycle





Supply Chain Risk Countermeasures

Opportunity to Target Surreptitiously



Consequence for Life & Mission

* Joint Federated Assurance Center (JFAC)
 **DoD Instructions in Place



Spectrum of Supply Chain Risks

Quality Escape

Product defect/ inadequacy introduced either through mistake or negligence during design, production, and post-production handling resulting in the introduction of deficiencies, vulnerabilities, and degraded life-cycle performance.

Reliability Failure

Mission failure in the field due to environmental factors unique to military and aerospace environment factors such as particle strikes, device aging, hot-spots, electro-magnetic pulse, etc.

Fraudulent Product

Counterfeit and other than genuine and new devices from the legally authorized source including relabeled, recycled, cloned, defective, out-of-spec, etc.

Malicious Insertion

The intentional insertion of malicious hard/soft coding, or defect to enable physical attacks or cause mission failure; includes logic bombs, Trojan 'kill switches' and backdoors for unauthorized control and access to logic and data.

Reverse Engineering

Unauthorized extraction of sensitive intellectual property using reverse engineering, side channel scanning, runtime security analysis, embedded system security weakness, etc.

Information Losses

Stolen data provides potential adversaries extraordinary insight into US defense and industrial capabilities and allows them to save time and expense in developing similar capabilities.

DoD Program Protection focuses on risks posed by malicious actors



Counterfeit Parts



Counterfeit / Clone Component Threat Space

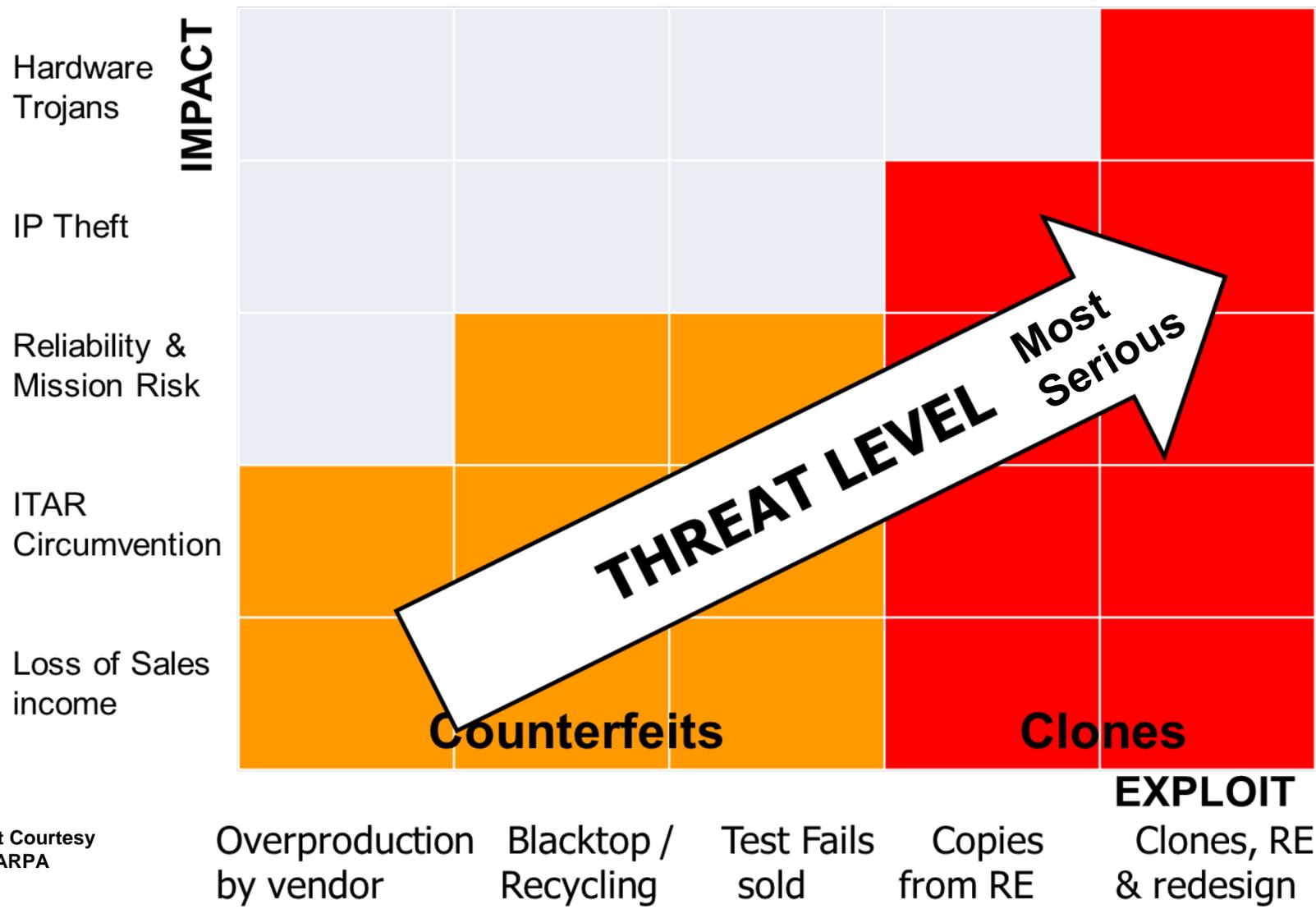


Chart Courtesy Of DARPA



Current and Emerging Requirements



- **DoDI 4140.67 DoD Counterfeit Prevention Policy**
 - Requires procurement of critical electronic parts from suppliers that meet risk-based criteria
 - Applies additional measures when such suppliers not available
- **National Defense Authorization Act**
 - Fiscal Year 2012 Section 818 – Detection and Avoidance of Counterfeit Electronic Parts
 - Fiscal Year 2013 Section 833 – Contractor Responsibilities in Regulations Relating to Detection and Avoidance of Counterfeit Electronic Parts
- **Emerging regulations**
 - FAR 2012-032 “Higher Level Quality Requirements”
 - DFARS 2012-D055 “Detection and Avoidance of Counterfeit Electronic Parts”
 - FAR 2013-002(proposed) “Expanded Reporting of Nonconforming Items”
 - DFARS 2014-005 (in draft) “Detection and Avoidance of Counterfeit Electronic Parts – Further Implementation”



GIDEP Reporting (Information Sharing Portal)



- **Most companies and agencies have some sort of “Quality Deficiency Reporting System”**
- **GIDEP is a way of linking the knowledge in these systems together for the “collective good”**
- **Mandatory reporting of non-conformances (including suspected or confirmed counterfeits)**
- **Modernize GIDEP system (entry; storage; retrieval)**
- **Efficient correlation of information**



<http://www.gidep.org/>



Joint Federated Assurance Center



Joint Federated Assurance Center (JFAC)



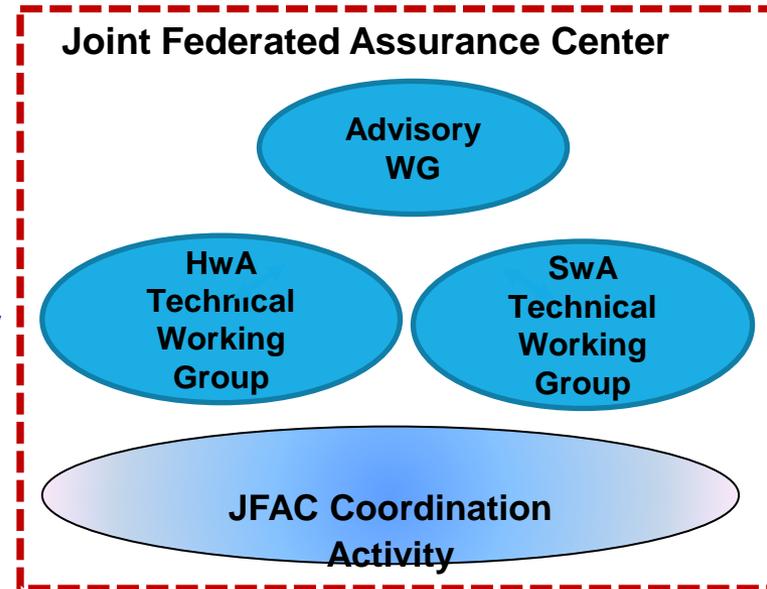
NDA 2014 directed DoD to “provide for the establishment of a joint federation of capabilities to support the trusted defense system needs...to ensure security in the software and hardware developed, acquired, maintained, and used by the Department”

For Hardware and Software Assurance:

- Establish a federation of capabilities to support program protection planning and execution
- Support program offices across the life cycle by identifying and facilitating access to expertise, capabilities, policies, guidance, requirements, best practices, contracting language, training, and testing support
- Coordinate needs and findings with research
- Procure, manage, and distribute enterprise licenses for assurance tools

Status:

- JFAC Charter has been staffed and is in-process for DEPSECDEF signature
- 937 Congressional Report in-process and on track
- Working the concept of operations, DoD assurance capability map, and capability gap analyses
- Initial capability on track for 2015





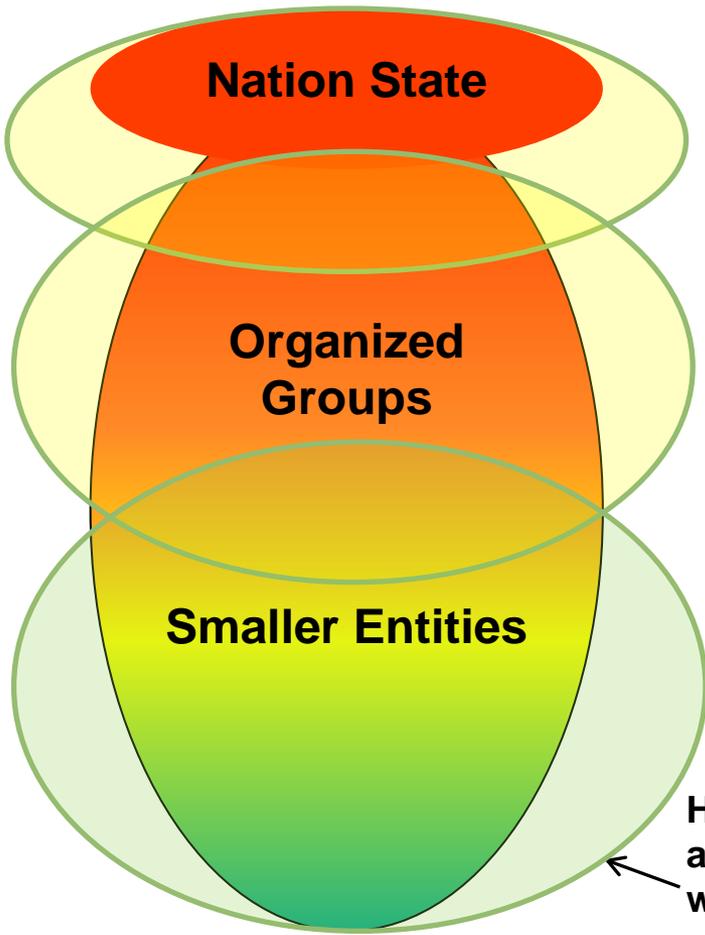
Hardware Threats and Mitigations

- We must better understand the SCOPE and NATURE of the threat

Tampered
Re-Manufactured

Clones
Substitutions

Re-used
Re-labeled
Test Rejects



Verifying proper construction and operation

- Scanning Electron Microscopy
- Special Electrical Test
- Laser Scanning Microscopy
- Transmission Electron Microscopy
- Time-of-Flight Secondary Ion
- Mass Spectrometry
- Verification and Validation (ASIS & FPGA)

Looking for internal identifiers

- Scanning Acoustic Microscopy
- Traditional Electrical Test
- Non-traditional Electrical Test

Looking for re-packaging

- Visual Inspection
- Solvents Testing
- X-Ray Fluorescence
- X-Ray Inspection

High percentage of fraudulent parts are found in this category, but that's where almost all assessment occurs

Chart Courtesy of NSWC Crane



Trusted Microelectronics



Problem Statement



Vulnerabilities in supply chain could lead to malicious logic insertions

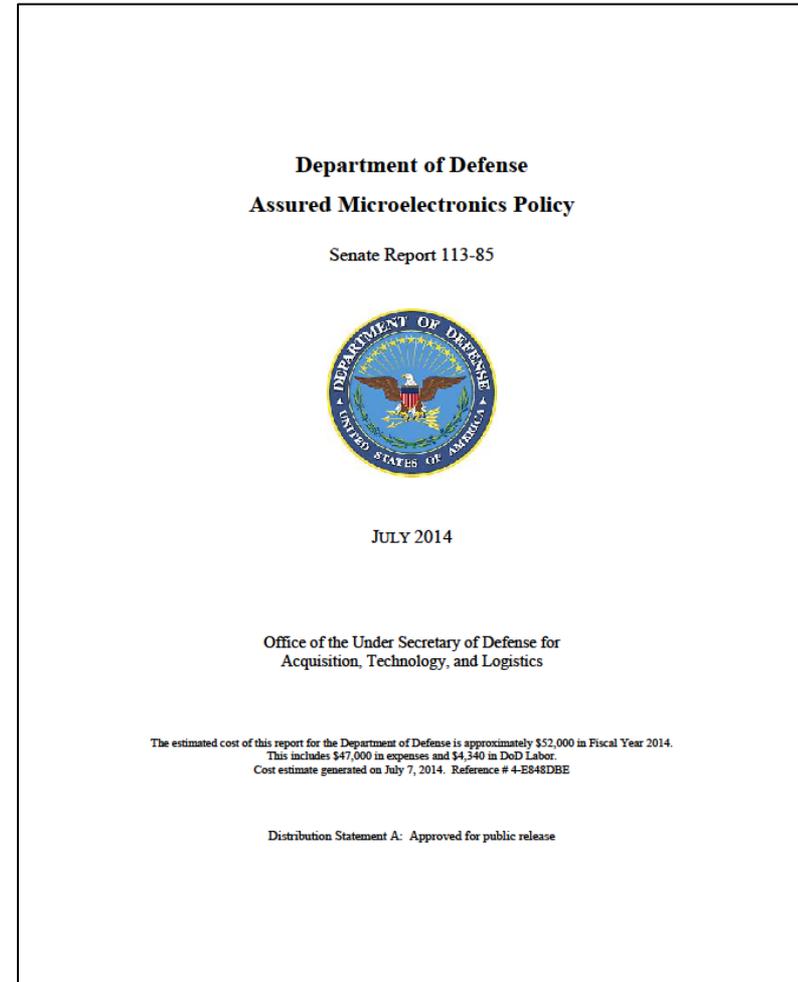
- **Current DoD-unique ASICs used in DoD systems are procured via a Trusted Supplier chain per DoD policy**
 - Accounts for approximately 10% of logic-bearing DoD Integrated Circuit (IC) products used in DoD systems
- **Approximately 72% of DoD ICs are non-ASICs; largely Field Programmable Gate Array (FPGA) devices**
 - DoD has no current trusted supply chain for FPGAs
 - FPGAs include COTS and Military grade products
 - Much of the FPGA value chain is off-shore, e.g., design, fabrication, programming services, testing and packaging
- **FPGAs that are programmed by DoD end-users may face Software Assurance (SwA) risks in FPGA bitstream programming tools, environment, and processes**
- **Bottom line: ASICs and FPGAs are not the only ICs of concern (must address more than ASIC foundry operations)**



Assured Microelectronics



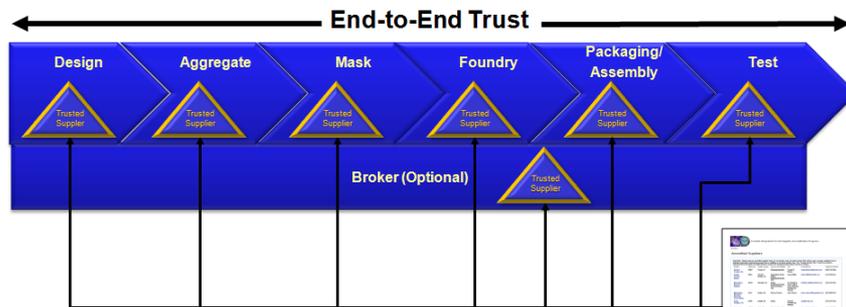
- **Beyond Application-Specific Integrated Circuits (ASICs)**
- **Identifying critical functions and components**
- **Analyzing risk and identifying mitigations**
- **Leveraging existing policies and guidance**



<http://www.acq.osd.mil/se/docs/DoD-Assured-Microelectronics-Policy-RTC-July2014.pdf>



Trusted Foundry Program

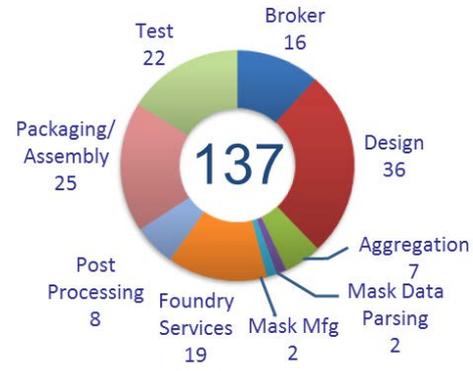


Supplier	Design	Aggregate	Mask	Foundry	Packaging/Assembly	Test
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						
16						
17						
18						
19						
20						
21						
22						
23						
24						
25						
26						
27						
28						
29						
30						
31						
32						
33						
34						
35						
36						
37						
38						
39						
40						
41						
42						
43						
44						
45						
46						
47						
48						
49						
50						

- **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 28 Aug 2014



Manufacturing



Aerospace Standard 6500 Manufacturing Management Program



- **AS 6500 Published Nov 13, 2014**
- **Goal**
 - Encourage the use of best manufacturing management practices aimed at promoting the timely development, production, modification, fielding, and sustainment of affordable products.
- **References SAE STD-0016 “Standard for Preparing a DMSMS Management Plan” and SD-22 “DMSMS Guidebook”**
- **DMSMS Para 5.4.1(c) requires:**
 - Development and implementation of a DMSMS Management Plan (entire program including support equipment)
 - Establishment of a risk-based DMSMS monitoring system
 - Identification of diminishing manufacturing sources and obsolete materials used or planned to be used in the program
 - Development of plans and procedures to mitigate the risk of obsolete parts



Assessing Manufacturing Risk

- **Interim DoDI 5000.02**

- “The Program Manager will ensure manufacturing and producibility risks are identified and managed throughout the program’s life cycle.”

- **DoD Risk Management Guide (Update Underway)**

- **Current practice: MRLs**

- A. Technology and the Industrial Base
- B. Design
- C. Cost and Funding
- D. Materials (Availability, SCM)**
- E. Process Capability and Control
- F. Quality Management
- G. Manufacturing Workforce
- H. Facilities
- I. Manufacturing Management

Version 11.3		14-Jun-12		DoD Manufacturing Readiness Levels (MRLs)			
Acquisition Phase		MSA	Material Solution Analysis (MSA)		Technology Development (TD)		
Technical Reviews			ASR	A	SRR/SFR	PDR	B
Thread	Sub-Thread						
Components, Sub-Assemblies and Sub-systems	D.1. Maturity	Material properties validated and assessed for basic manufacturability using experiments.	Projected materials have been produced in a laboratory environment.		Materials have been manufactured or produced in a prototype environment (may be in a similar application/program). Maturation efforts in place to address new material production risks for technology demonstration.	Material maturity verified through technology demonstration articles. Preliminary material specifications in place and material properties have been adequately characterized.	Material maturity build. Material
	D.2. Availability	Material scale-up issues identified.	Projected lead times have been identified for all difficult to obtain, difficult to process, or hazardous materials. Quantities and lead times estimated.		Availability issues addressed for prototype build. Significant material risks identified for all materials. Planning has begun to address scale-up issues.	Availability issues addressed to meet EMD build. Long-lead items identified. Components assessed for future DMSMS risk.	Availability issue. LRP builds. Led identified and mitigation strat place.
	D.3. Supply Chain Management	Initial assessment of potential supply chain capability.	Survey completed for potential supply chain sources.		Potential supply chain sources identified and evaluated against support requirements.	Lifecycle Supply Chain requirements updated. Critical suppliers list updated. Supply chain plans in place (e.g. teaming agreements, etc.) supporting an EMD contract award.	Effective supply chain processes defined. Plan development. Assess (ber) supply chain capabilities.

Example: “Components assessed for future DMSMS Risk”

<http://www.dodmrl.org>



Systems Engineering: Critical to Defense Acquisition



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

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