Trusted Sources, Supply Challenges and Solutions



Sydney Pope AT&L (Industrial Policy) February 12, 2010



Presentation Outline

- Trusted Microcircuit Challenge
- Cyber-Security Strategy
- Policy Development
- Counterfeiting Implications
- Government and Industry Interactions
- Thoughts for Consideration



The Microelectronics Challenge

Increased DoD use / reliance for ("Smart" systems)

- Essential technology for all military missions
 - Strategic, tactical, C4I, special ops
 - "Critical" DoD technology
- Enabling technology for adaptive operations,
 transformational opportunities & spiral development

Extended system life cycles (20 – 40 years)

- Rapidly evolving, expanding missions
 - Asymmetric threats
 - New capability requirements
- Increased system reliability and maintainability issues
- Diminishing Manufacturing Sources (DMS)
 - Obsolescence cycles of 18 months or less
 - Over 90% of all DoD DMS cases are electronics

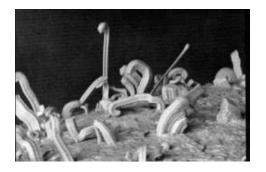
Commercial market dictates the technology

- Very high volumes for short terms
- Off shore manufacturing
- Lower environmental quality thresholds & EU RHOS (lead-free solder) mandates











Trust Sources are Element of Cyber-Security Strategy

Mission critical IT and Weapon Systems

Systems Assurance Addressed in DODI 5200.39 Revision

Defines broadly what needs to be done

- Critical Program Information defined by taking into account horizontal protection
- Covers confidentiality, but also defines technology, components and material needing protection
- Program Protection Plan defines strategy for employing mitigating approaches for protecting CPI



Department of Defense INSTRUCTION

NUMBER 5200.39 July 16, 2008

USD/I

SUBJECT: Critical Program Information (CFI) Protection Within the Department of Defense

References: See Enclosure 1

- PUKPOSE. This Instruction:
- Reissues DoD Directive 520039 (Reference (a)) as a DoD Instruction in accordance with the guidance in DoD Instruction 5025.01 (Reference (b)) and the authority in DoD Directive 5143.01 (Reference (c)).
 - Establishes policy for the protection of CPI.
- (2) Issues policy and assignment possibility for counterintelligence (CI), Intelligence, Security, and Systems Engineering support for the identification and protection of CPI.
- (3) Assigns responsibilities to DoD Components relating to the identification of CPI and the implementation of plans for its protection.
- b. Provides policy on and implements relevant parts of DoD Directive 5000.01 (Reference (di)) and DoD Instruction 5100.2 (Reference (e)).
 - c. Authorizes the issuance of additional guidance, consistent with Keference (b).
- d. Continues to authorize the publication of DoD 52(0.1-M (Reference (3) as the conversabing implementing issuance for this Instruction until such time that it is replaced. Where inconsistencies exist between this Instruction and Reference (f), this Instruction shall supercede.
- e. Supplements existing policies and guidance related to the security of DoD personnel, information, resources, installations, and operations to include DoD contractors performing work or supporting a DoD research, development, and acquisition (RDA) effort (e.g., DoD Directive 5205.00 (Reference (g)), DoD 5200.1-R (Reference (g)), or DoD 5300.8-R (Reference (g))).
- APPLICABILITY. This Instruction applies to:

Critical Program Information (CPI) Protection Within The Department Of Defense, 5200.39, Issued 7/16/2008



Trust Sources are Element of **Cyber-Security Strategy**

Mission critical IT and Weapon Systems

Systems Assurance Addressed in DODI 5200.39 Revision



NUMBER 5200.39 July 16, 2008

Defines broad

- needing
- Program for emplo

protecting CPI

Related Cyber Security cases:

- Critical P • DFARS Cases 2008-D028 & FAR

taking int Case 2009-030 on Safeguarding

Covers c Unclassified Information

technolog • FAR Case 2009-032, "Sharing **Cyber Threat Information**"

ence (a)) as a DoD Instruction in accordance with reme (b)) and the authority in DoD Directive

Protection Within the Department of Defense

lity for counterintelligence (CI), Intelligence, the identification and protection of CFI.

aponents relating to the identification of CPI and

ant parts of DoD Directive 5000.01 (Reference

dance, consistent with Reference (b)

DoD 5200.1-M (Raference (3)) as the metion until such time that it is replaced. Where od Reference (f), this Instruction shall supersede.

ace related to the security of DoD personnel,

nons to include DoD contractors partnerning work or supporting a DoD research, development, and acquisition (RDA) effort (e.g., DoD Directive 5205.02 (Raference (g)), DoD 5200.1-R (Raference (h)), or DoD 5000.08-R (Raference (i)))

2. APPLICABILITY. This Instruction applies to:

Critical Program Information (CPI) Protection Within The Department Of Defense, 5200.39, Issued 7/16/2008

1/14/2010

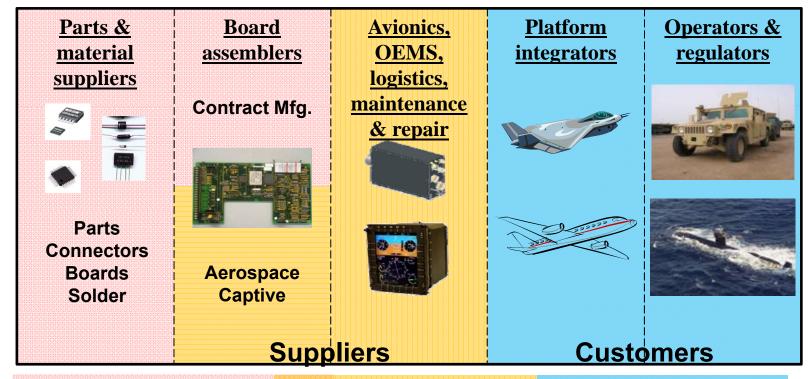


Supply Chain Risk Management



• Executive and Legislative Guidance CNCI Initiative 11 - Directed Improved Supply Chain Risk Management 1-8-08

...but in reality





Trust Microelectronics Policy

DepSecDef & AT&L 2004 Policy Letters

- Trust is minimum requirement for defense systems
- **Beyond critical Application** Specific ICs, policy needed that provides a comprehensive, viable, cost-effective, and realistic approach for preserving system-level trust
- Trust should include multilayered defense-in-depth as a practical strategy involving people, technology, and operations



OFFICE OF THE SECRETARY OF DEFENSE WASHINGTON, DC 20301



MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS DIRECTOR, DEFENSE INFORMATION SYSTEMS

AGENCY DIRECTOR, DEFENSE INTELLIGENCE AGENCY

DIRECTOR, NATIONAL GEOSPATIAL-INTELLIGENCE

DIRECTOR, NATIONAL SECURITY AGENCY DIRECTOR, DEFENSE SECURITY SERVICE DIRECTOR, NATIONAL RECONNAISSANCE OFFICE DIRECTOR, MISSILE DEFENSE AGENCY DIRECTOR, DEFENSE ADVANCED RESEARCH

PROJECTS AGENCY

SUBJECT: Interim Guidance on Trusted Suppliers for Application Specific Integrated

The Department of Defense is implementing a "Defense Trusted Integrated Circuits Strategy (DTICS)," as approved by the Deputy Secretary of Defense on October 10, 2003. Trust is the confidence in one's ability to secure national security systems by assessing the integrity of the people and processes used to design, generate, manufacture, and distribute national security critical components (i.e., microelectronics). The DTICS is intended to address the Department's concerns that defense systems relying upon advanced integrated circuits (ICs) for critical capabilities may be vulnerable or compromised if not produced in a trusted manner, thereby jeopardizing our current technical advantages. Consequently, the Department is acting quickly to address this vulnerability and threat to our warfighting capabilities.

As a first element of this strategy, policy is being developed that shall require all trusted systems of category I (Attachment 1) to employ only trusted foundry service(s) to fabricate their custom designed ICs. Programs that wish to seek a waiver of this policy are required to perform a thorough risk and vulnerability assessment of the fabrication of their critical ICs and submit this assessment, with a mitigation strategy, to OUSD (AT&L) for approval. The key metric to be considered is the protection of sensitive applications, where a functional compromise would cause severe interference or stoppage of warfighter operations and/or direct mission support operations. Some of these trusted systems that use foundry services have already been identified (Attachment 2). It is essential that these ICs be fabricated or obtained from sources that have been certified as trusted. This policy is a logical extension of recently implemented Information Assurance (IA) policy contained in the 8500 series of DoD Directives.



1/14/2010



Trusted Supplier Program

- Interim Guidance Jan 04, required highly sensitive acquisitions to manufacture ASICs in a trusted foundry.
 - DoD/NSA establish a funded Trusted Foundry Program
 - IBM established early on as trusted ASIC source
 - DMEA Certified 31 suppliers (design, foundry, pkging) participating (1/2010)
 - Has not fundamentally changed how most systems acquire





Section 254 Trusted Def Systems*

(FY09 Defense Authorization Act)

Vulnerability Assessment

Verification Methods

Integrated Strategy

Acquisition Policy

- Identify (ID)
 program
 vulnerabilities
 within IT &
 electronic
 systems
- Prioritize potential vulnerabilities and effects

- ID verification methods for verifying microelectronic circuit trust
- •ID additional R&D needed
- ID Lead person(s)
 to develop integrated
 strategy
- Develop integrated strategy for managing supply chain risk
- Formalize strategy for ensuring dependable, continuous, long term access and trust of mission-critical circuits, foreign and domestic sourced

PCB trust is a concern as well

* Section 256 Requires DoD to Establish Printed Circuit Board Exec. Agent



Design Verification





- DARPA developing new techniques to verify IC designs perform only operation intended
- FPGAs & ASICs primary focus
- Destructive methods only way now available to confirm design
- Malicious circuits can be inserted in OEM ICs and Counterfeits

The TRUST Program Will Enhance the Trustworthiness of IC's Regardless of Where They are Manufactured

1/14/2010



Trust Implications From Counterfeiting

- Tampering --- To Engage in Espionage or Sabotage
- Counterfeiting--→ Economics --→ Greed

Both Lead to Intentionally Compromised Devices

- May be Impossible to Detect
- Can Jeopardize Both Mission and Life

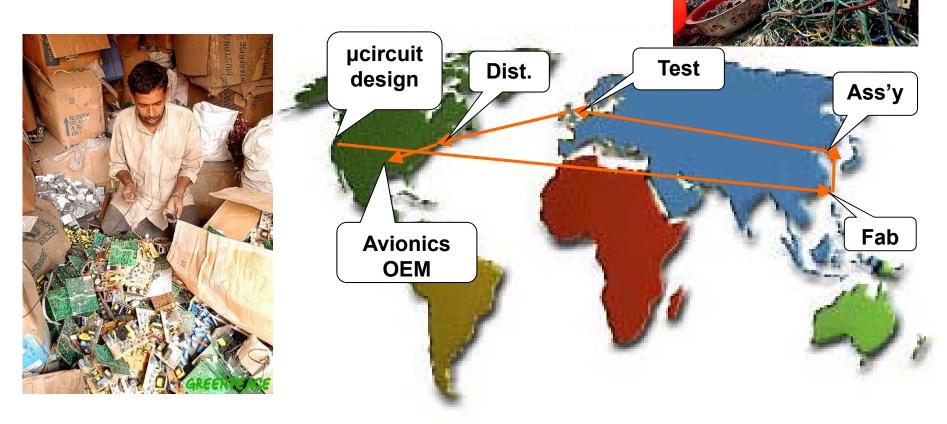
Ways To Address Counterfeiting Risk:

- Buy from Established Sources (OEMs, Authorized Distributors, etc.)
- Conduct Independent Testing and Inspection
- Establish Controls and Common Language and Methods for Performance Requirements and Criticality of End Use
- Adopt Traceability Mechanisms (Tagging, etc.)
- Report instances of Counterfeiting to law enforcement and GIDEP



"Typical" Microcircuit Product Flow

The microcircuit chain is....circuitous. The number of potential combinations of links is large, and growing. Ability to "control" shrinking.



12



BusinessWeek



October 2, 2008

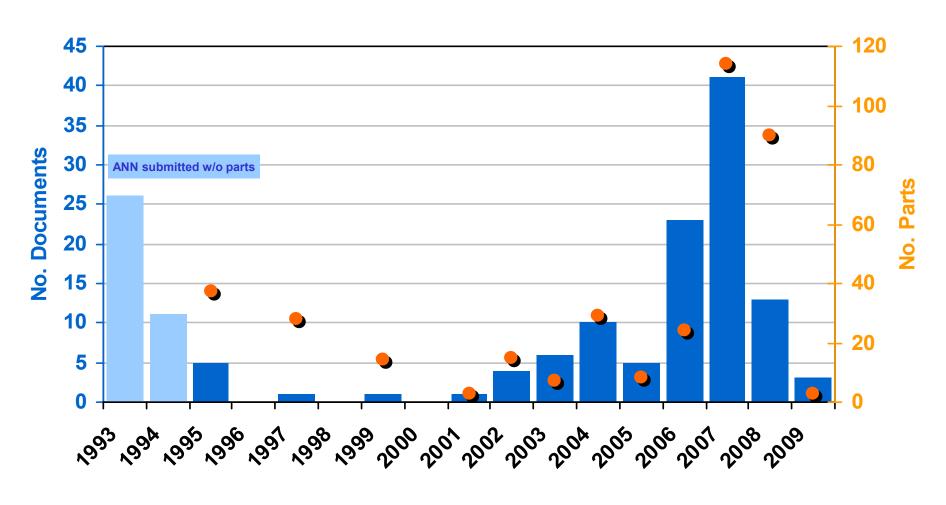
- General William G.T. Tuttle Jr., former chief of the Army Materiel Command and now a defense industry consultant, agrees: "What we have is a pollution of the military supply chain." Much of that pollution emanates from the Chinese hinterlands.
- A BusinessWeek analysis of a contracting database identified at least 24 active brokers that list residential homes as their place of business. Several have won chip contracts for "critical applications," which the Pentagon defines as "essential to weapon system performance...or the operating personnel." In many cases these entrepreneurs comb Web sites such as brokerforum.net and netcomponents.com, which connect them with traders in Shenzhen and Guiyu.
- The brokers sell either directly to Pentagon depots or via suppliers to defense contractors such as BAE.

13



GIDEP Counterfeit Reporting

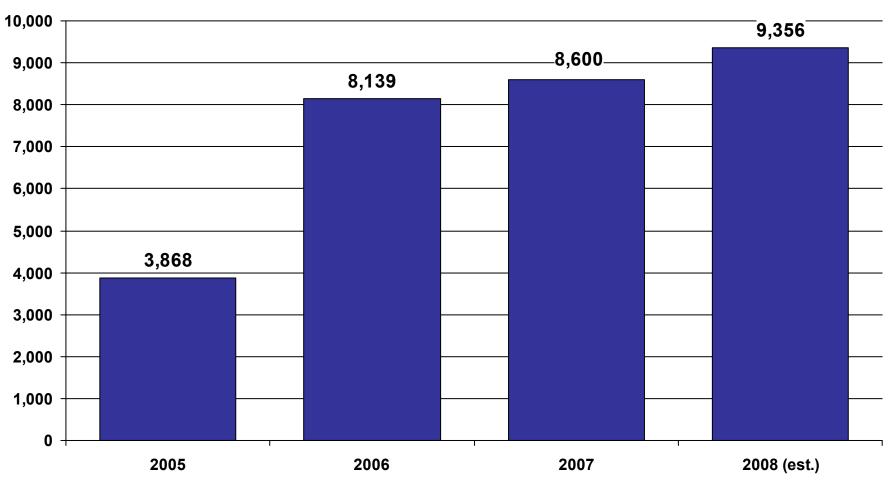
Number of Documents & Parts





Total Counterfeit Incidents: OCMs, Distributors, Board Assemblers,

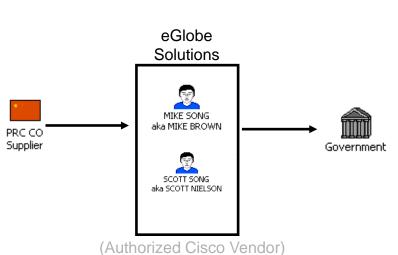
Prime/Sub Contractors 2005 - 2008



Source: U.S. Department of Commerce, Office of Technology Evaluation, Counterfeit Electronics Survey, Nov 2009. (Report published Jan 2010)



CISCO Router Case





eGlobe Solutions Inc.

- •May 2003 July 2005: Sold \$788,000 of counterfeit equipment
- •November 2006 Indictment: Conspiracy, Mail Fraud, Counterfeiting
- Sold to: DoD, GSA, defense contractors, power companies



FAR Case 2008-019; Authentic Info Tech Products, 73 Fed. Reg. 68373 (Nov 18, 08)

- DoD, GSA, & NASA Sponsored Proposal
 Post-CISCO 2004 Router Counterfeiting Event
- OEM in "Gatekeeper" role to assure Hardware & Software
- May extend to components / other
- Offeror represents products as Authentic / Not Counterfeit
- No limitation on Contractor liability
- Industry initial response negative

B4LLING CODE 6560-50-P

DEPARTMENT OF DEFENSE

GENERAL SERVICES ADMINISTRATION

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

48 CFR Parts 2, 4, 12, 39, and 52

[FAR Case 2008-019; Docket 2008-0001; Sequence 1]

RIN 9000-AL11

Federal Acquisition Regulation; FAR Case 2008–019, Authentic Information Technology Products

AGENCIES: Department of Defense (DoD), General Services Administration (GSA), and National Aeronautics and Space Administration (NASA).

ACTION: Advance notice of proposed rulemaking and public meeting.

SUMMARY: The Civilian Agency Acquisition Council and the Defense Acquisition Regulations Council (Councils) are seeking comments from both Government and industry on whether the Federal Acquisition Regulation (FAR) should be revised to include a requirement that contractors selling information technology (IT) products (including computer hardware and software) represent that such products are authentic. The Councils are also interested in comments regarding contractor liability if IT products sold to the Government, by contractors, are not authentic. Additionally, the Councils are seeking comments on whether contractors who are resellers or distributors of computer hardware and software should represent to the Government that they are authorized by the original equipment manufacturer (OEM) to sell the information technology products to the Government. Finally, the Councils invite comments on [1] whether the measures contemplated above should be extended to other items purchased by the Government; and (2) whether the rule should apply when information technology is a component of a system or assembled product.



Diminishing Manufacturing Sources and Material Shortages ATL Memo, August 16, 2004



Total Life Cycle Systems Management Executive Council to:

- 1. Define DoD microcircuit requirements (short and long term) and develop a technology roadmap for all systems
- 2. Develop predictive techniques for testing, configuration database management, preferred parts lists, and preferred suppliers to control product development, and redesign
- 3. Manage the industrial base and organic capability necessary to assure product availability
- 4. Optimize relationship between organic supply and redesign repair capabilities
- 5. Change organization, policy, procedures and design rules to fulfill the above





A daunting task





Microcircuits and Semiconductors (FSC 5962/5961)



95,260 Individual Material Numbers (NSNs)

Within the last year:



12,500 (13.1%) NSNs are Active

- 68,400 Orders per year
- 447,000 Parts
- \$26.6M Annual Demand Value

4,300 (5%) NSNs Drive

- 55,700 Orders per year
- 351,000 Parts
- \$23.6M Annual Demand Value

Managing a high risk environment

- DoD does not drive the market
- Aging weapon systems leading to obsolescence
- Large distributor network, few OEMs



ors

ply

- DSCP us distribut
- DSCC has of Integral
 - Both m
 - Franch
 - Status

Related IPT:

OSD initiated Dec 09
 Countering Counterfeits Tiger
 Team to Develop in 90-days
 DoD-Strategy for Addressing
 Electronic System Risk

Defense Logistics Agency Joint-Service Counterfeit IPT, initiated April 09



Looking into all commodity areas



Draft AIA Plan of Action

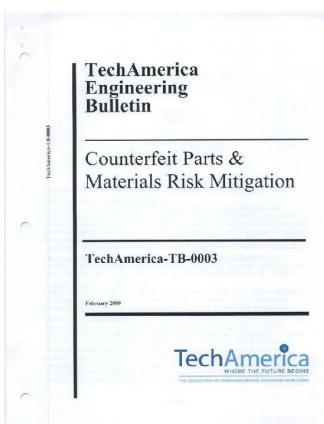
To Prevent introduction of counterfeits in aerospace, space, and defense, the Counterfeit Parts Integrated Project Team (IPT) proposes (as of Aug 4, 09)

- Create standards to manage counterfeit risk w/o sacrificing benefits of buying commercial products
- Enforcement of Laws to avoid counterfeit introduction in the U.S.
- 3. Use GIDEP as forum for receiving/disseminating counterfeit reports
- 4. Government relieve purchaser of counterfeits from payment and retain as evidence
- 5. Fund approaches to eliminate/mitigate use of obsolete components
- 6. DoD Supply Centers, Depots and Arsenals apply preference for OCM or authorized/franchised distributors, and apply countermeasures when buying from brokers
- 7. Provide training to increase awareness of counterfeit risk

21



Industry Published Documents



"...ensure that only new and authentic materials are used in products delivered...only purchase from **Original Component** Manufacturers (OCMs), franchised distributors, or authorized aftermarket manufacturers... present compelling support procured are authentic/conforming parts."

SAE Aerospace AEROSPACE STANDARD	S4E AS5553
	Issued 2009-04

RATIONA

This standard was created in response to a significant and increasing volume of counterfeit electronic parts entering the aerospace supply chain, posing significant performance, reliability, and safety risks.

This standard was created to provide uniform requirements, practices and methods to mitigate the risks of receiving an installing counterfeit electronic parts.

EODEMO

To assure customer satisfaction, aerospace industry organizations must produce, and continually improve, safe, reliable products that meet or exceed customer and regulatory authority requirements. The globalization of the acrospace industry and the resulting diversity of regional/mational requirements and expectations has complicated this objective. End-product organizations face the challenge of assuring the quality and integration of product purchased from suppliers throughout the world and at all levels within the supply chain. Aerospace suppliers and processors face the challenge of delivering product to multiplic customers having varying outsility expectations and requirements.

This document standardizes requirements, practices, and methods related to: parts management, supplier management procurement, inspection, test/evaluation, and response strategies when suspect or confirmed counterfeit parts at discovered.

SAE Technical Standards Board Rules provide that: "This report is published by SAE to advance the state of technical and engineering sciences. The use of this report entirely voluntary, and its applicability and sustability for any particular use, including any patient infringement arising therefore, is the cole responsibility of the use? ASE reviews existing therefore, is determined to the property of the prop

All rights reserved. No part of this publication may be reproduced, stored in a retrieval substonce or otherwise, without the prior written permission of SAE.

at of this publication may be reproduced, stored in a retrieval or otherwise, without the prior written permission of SAE.

TORDER: Tel: 877-605-7323 (Inside USA and Canada)

Tol: 774-775-4970 (wreded USA)

Fax: 724-776-0790
Email: CustomerService@
http://www.sae.org

satem or transmitted, in any form or by any means, electronic, mech SAE values your input. To provide feedback on this Technical Report, please visit, http://www.sae.org/technical/standards/AS5553

1/14/2010



Thoughts for Consideration

- Cyber security, trust and counterfeit component risk jeopardizing IT, mission and life-critical systems
- DoD and industry share interrelated SCRM and DMSMS challenges
- Acquisition and sustainment solutions need to be worked simultaneously and collaboratively

Consensus and leadership is needed to be successful