DOD Trusted Foundry Program

Ensuring "Trust" for National Security & Defense Systems

NAVAIR DMSMS Branch
January 9th, 2013

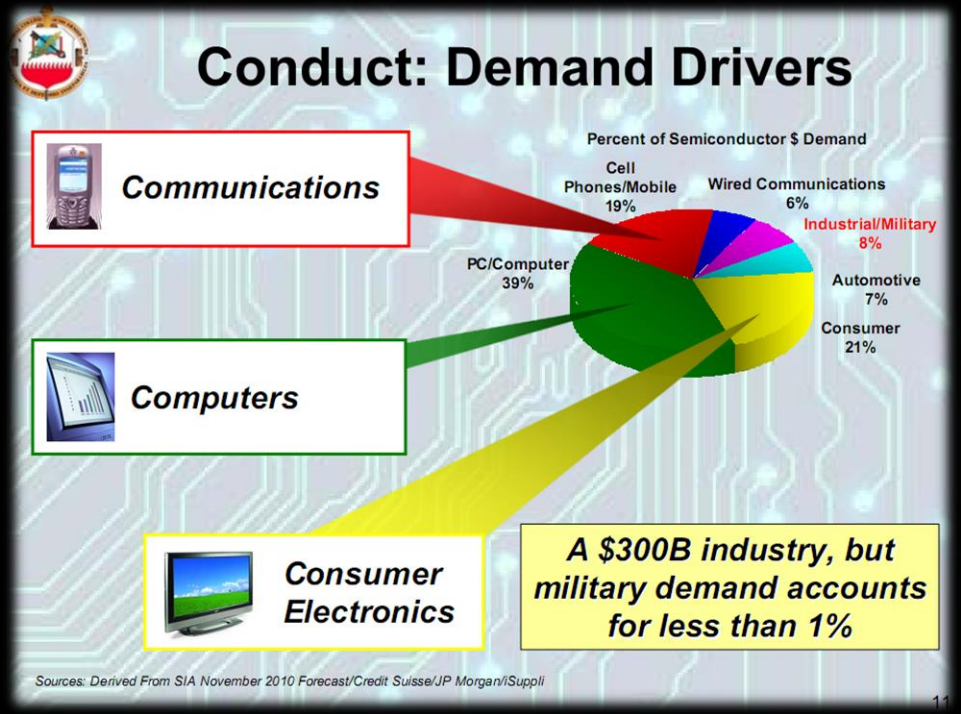
Catherine Ortiz
On behalf of the Trusted Foundry Program

Today's Discussion

- Global landscape for semiconductors
- Growing vulnerability in DoD supply chain
- The department's response to the situation
- The availability of products and services from a robust, domestic, Trusted supplier industrial base

Globalization of Microelectronics

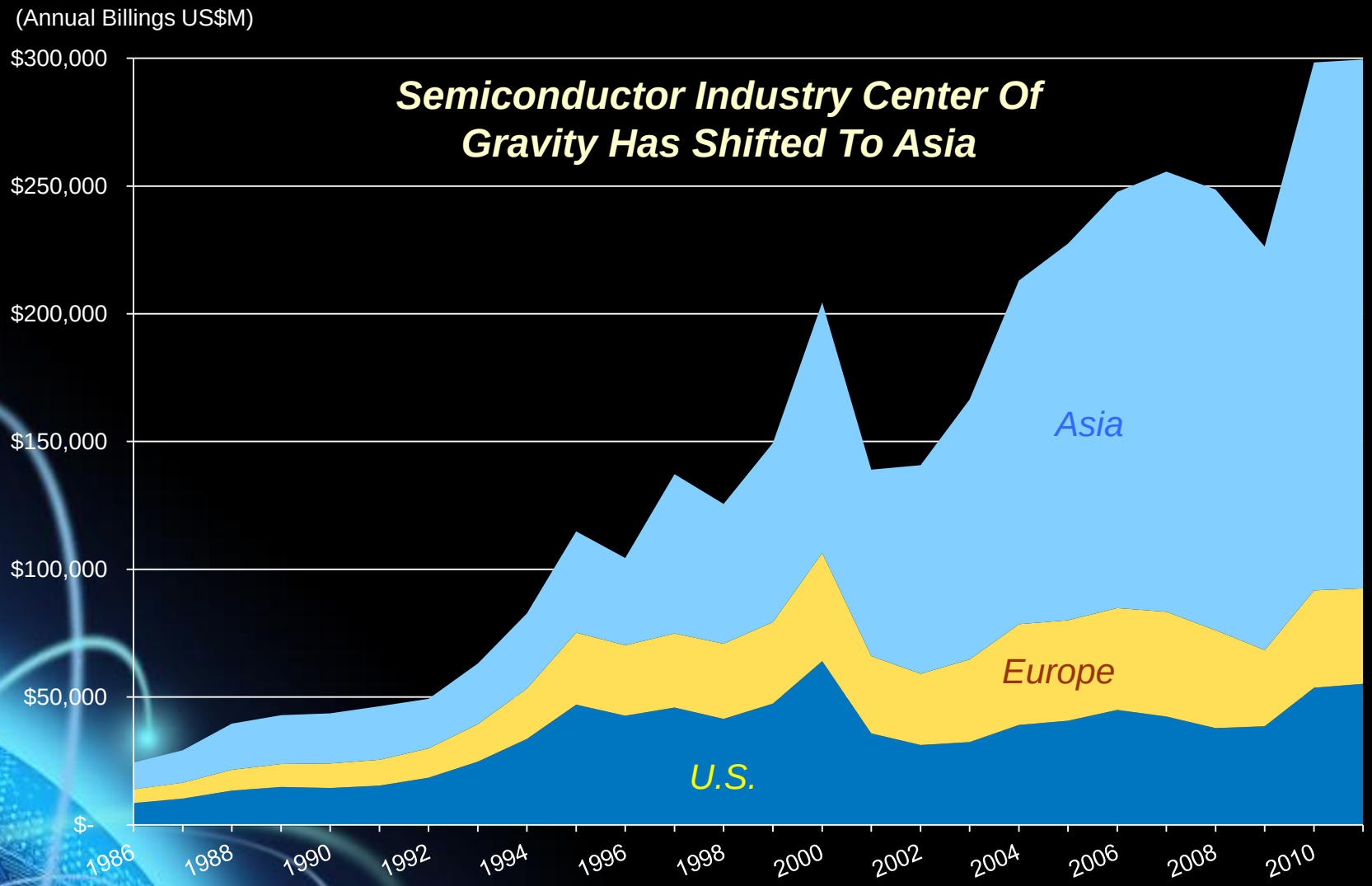
- Consumer electronics drivers
  - Large volumes
  - Short life cycles
- DoD requirements in contrast
  - Low volume
  - Long acquisition cycles, sustainment
- Migration of manufacturing to unsecure locations



Risks to DoD

Loss of access to state-of-the-art technologies
Loss of military critical intellectual property
Counterfeit chips
Insertion of malicious circuitry

Microelectronics Supply Threat



Source: World Semiconductor Trade Statistics, 2011 Blue Book

The Threats

Trojan Horses

Malware

IP Siphoning

Backdoors

Counterfeiting

Kill Switches

Denial of Service

Bot-Nets

Viruses

Reverse Engineering

Phobos-Grunt Downed by Bad Chips?

- Fell to Earth on 15 January 2012 [1]
  - "Failure mechanism attributed to the simultaneous disabling of two identical chips in the dual-computer control system, causing both to restart simultaneously."
  - "… the specific component identified in the report as the likely locus of the double-hardware failure—the WS512K32, which is a single-package assembly of SRAM totaling 512 kilobytes"
  - Press reports suggest that investigators thought the chip failures were a result of counterfeit components—lesser circuits labeled with higher performance qualities.
- "You must trust your supplier for the quality and integrity of your integrated circuits
  - You cannot test in the necessary quality and integrity

Photo: ROSCOSMOS/EPA/Landov
Waiting its Turn: The Phobos-Grunt probe before being loaded onto a rocket for launch on its failed trip to Mars.

[1] Did Bad Memory Chips Down Russia's Mars Probe? Moscow blames radiation wreckage on an SRAM chip, but does it add up? James Oberg, February 2012.

Trusted Foundry Program

- The Trusted Foundry Program (TFP) was established as a joint effort between Department of Defense and National Security Agency . . . *in response to Deputy Secretary of Defense Paul Wolfowitz's 2003 Defense Trusted IC Strategy memo*
  - Program is administrated by NSA's Trusted Access Program Office (TAPO)
  - DoD component resides in the Office of the Secretary of Defense, ASD R&E and is managed by Defense Microelectronics Activity (DMEA)
- By the end of the program in FY2013, DoD will have invested >$700M to ensure access to microelectronics services and manufacturing for a wide array of devices with feature sizes down to 32nm on 300 mm wafers

Program provides national security and defense programs with access to semiconductor integrated circuits from secure sources

Trusted Supplier Definition

Trusted Sources will:

- Provide an assured “Chain of Custody” for both classified and unclassified ICs,
- Ensure that there will not be any reasonable threats related to disruption of supply,
- Prevent intentional or unintentional modification or tampering of the ICs, and
- Protect the ICs from unauthorized attempts at reverse engineering, exposure of functionality or evaluation of their possible vulnerabilities.

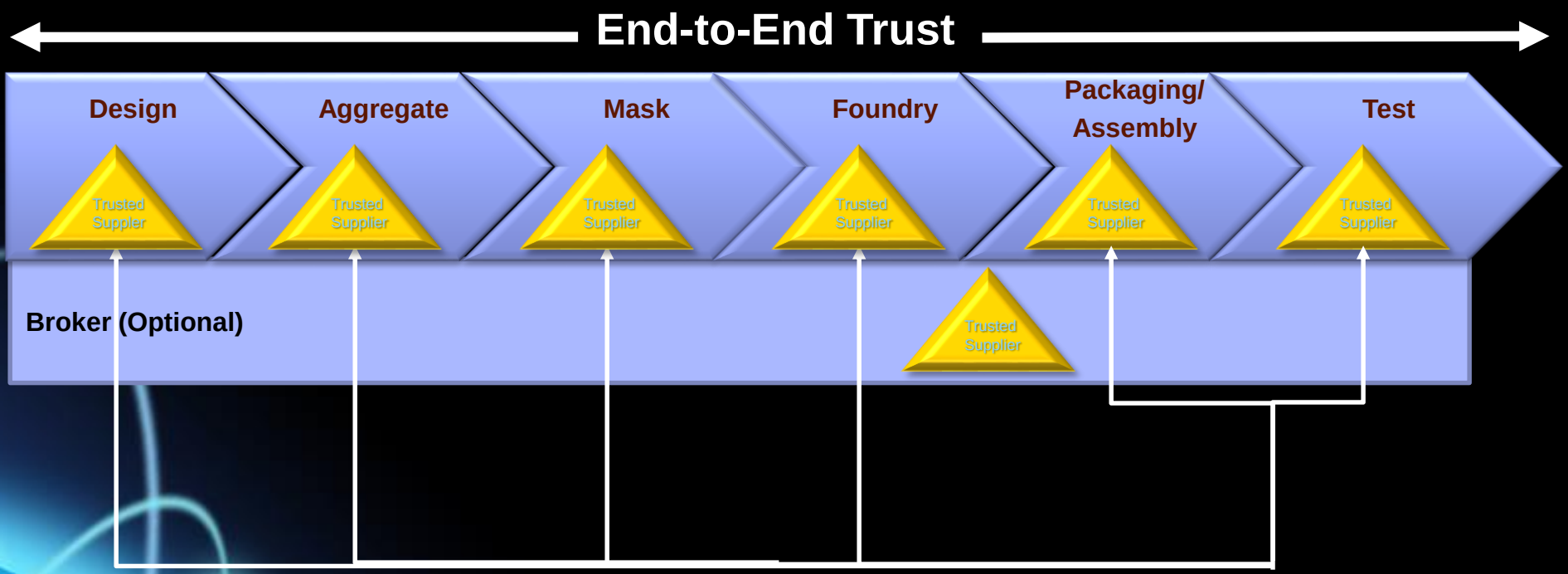
“Trust is the confidence in one’s ability to secure national security systems by assessing the integrity of the people and processes used to design, generate, manufacture, and distribute national security critical components”

A Trusted Supply Chain

- Trusted Foundry Program was originally implemented as a long term arrangement with IBM to secure access to leading-edge foundry technology
  - It was soon recognized that offering only IBM's capabilities left gaps in the trusted microelectronics supply chain
  - Program was broadened to include other microelectronics suppliers to increase competition and ensure the entire supply chain could be trusted
- Trusted supplier accreditation plan expanded the ranks of suppliers capable of providing trusted services for leading-edge, state-of-the-practice and legacy parts by certifying that suppliers meet a comprehensive set of security and operations criteria

Today, 55 suppliers are accredited to provide services ranging from design - - fab - - mask manufacturing - - packaging & testing

Trusted Integrated Circuit Supply Chain

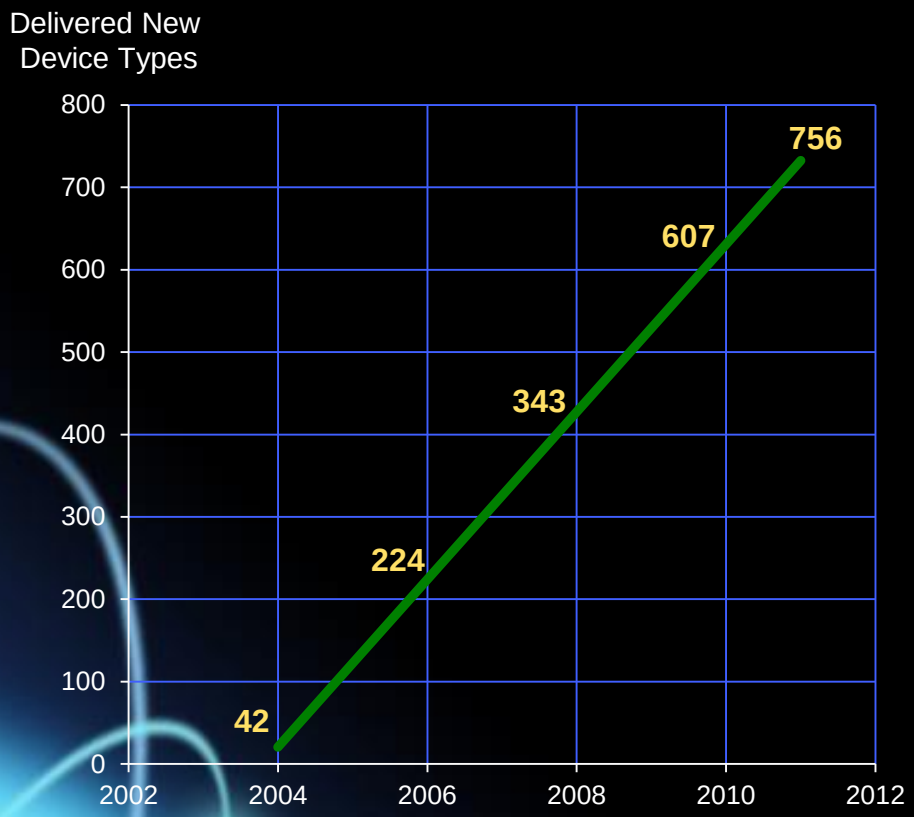


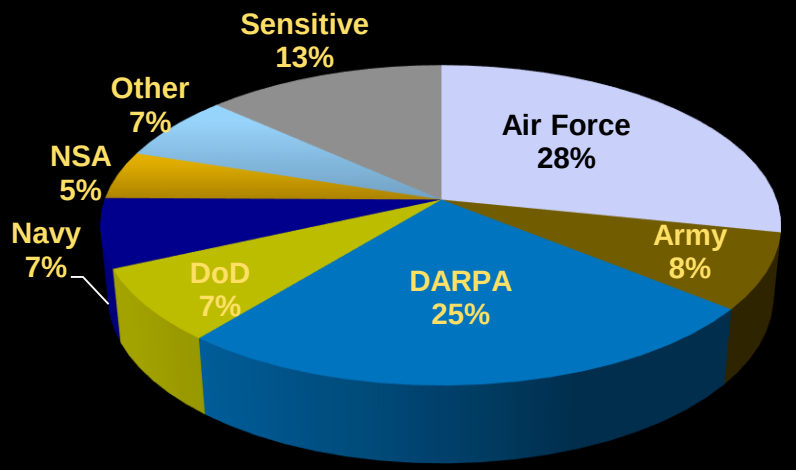
ISO 9001 Paradigm

IBM Trusted Foundry Contract

- Formally accredited (security/capability), leading-edge facilities, technology and people
- Government access to capacity as “Gold Customer” - - at commercial pricing
- Access to all IBM proprietary libraries, processes and R&D; common IP licensed for defense community use
- Demand is aggregated from across the customer community for multiple program wafer (MPW) runs and prototyping production
- Single POC (NSA-TAPO) simplifies & reduces administrative burden and complexity for users
- Government maintains a secure catalog of all designs - - available to all defense/intel PMOs

Growth in Use of MPW Access Model with IBM

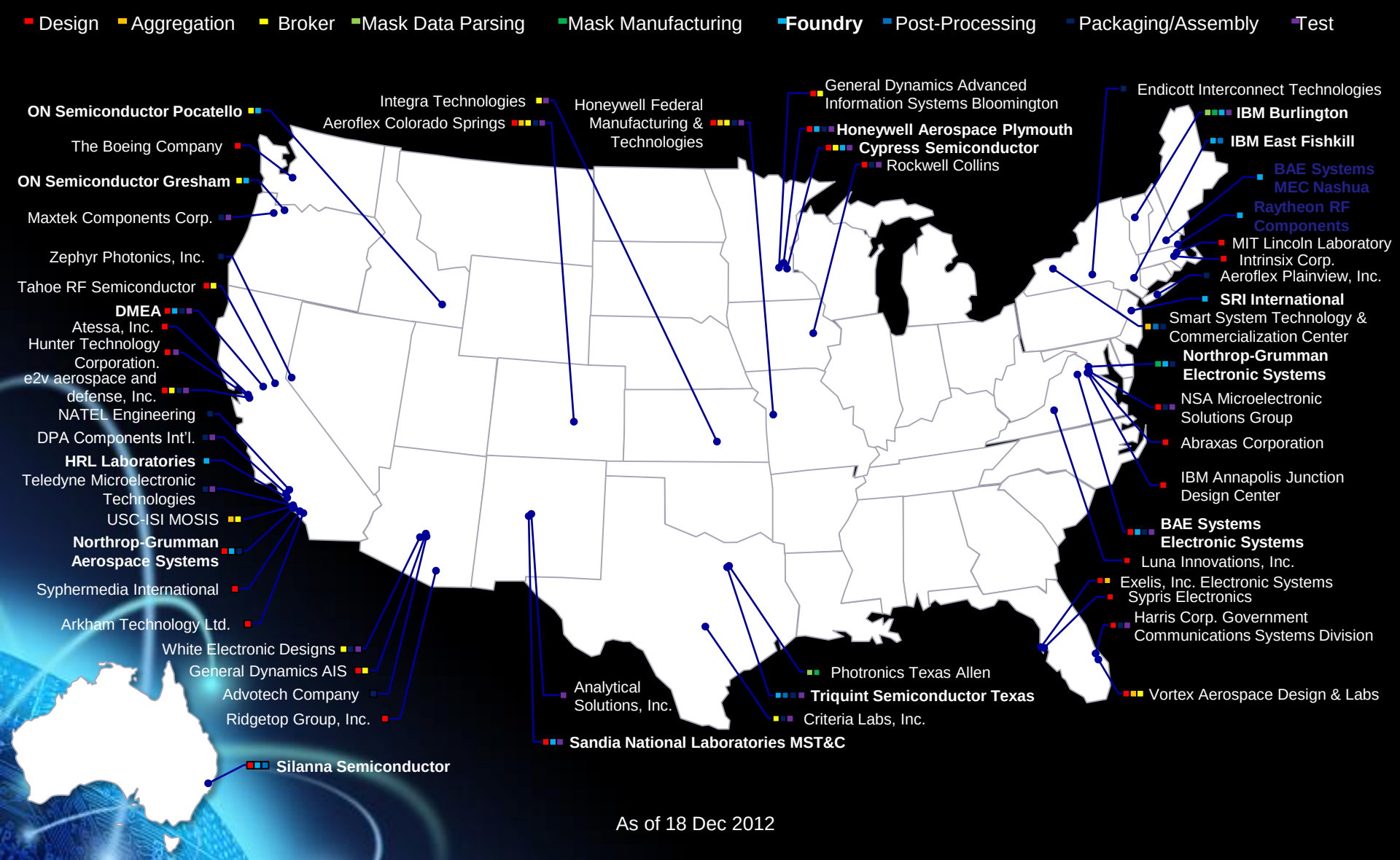




DoD MPW Access Program Use FY2011

The aggregation of many designs into a single manufacturing Multiple Project Wafer Run (MPW) significantly reduces costs for each program

55 Trusted Suppliers



As of 18 Dec 2012

Products and Services Offered

- Trusted packaging design, test and assembly
- MEMS
- Trusted product evaluations such as failure analysis, counterfeit design evaluation, environmental testing, trade studies, non-destructive testing . . .
- RAD HARD microcircuit design and fabrication
- Trusted microcircuit emulation
- Anti-cloning protection
- Trusted photomask development and parsing
- Military-grade cryptography Type 1 enabled IP cores
- Trusted ASIC and FPGA design and broker services

Trusted Domestic Sources are Available for a Full Range of Microelectronics Design, Production, and Test For leading-edge, state-of-the-practice, & legacy microelectronics

Trusted Microelectronics Options

Trusted IC Requirement

State-of-the-Practice or Legacy?

Leading Edge?

Determine Trusted products and services needed

Review Trusted Accredited Suppliers (TAS) capabilities

Supplier services and POCs listed on DMEA website

Initiate direct engagement with one or more TAS

- OR -

Initiate direct engagement with aggregator or broker

Explicitly request Trusted Flow at each stage of engagement

TAPO Trusted Access Program Office

Government Sponsor

IBM

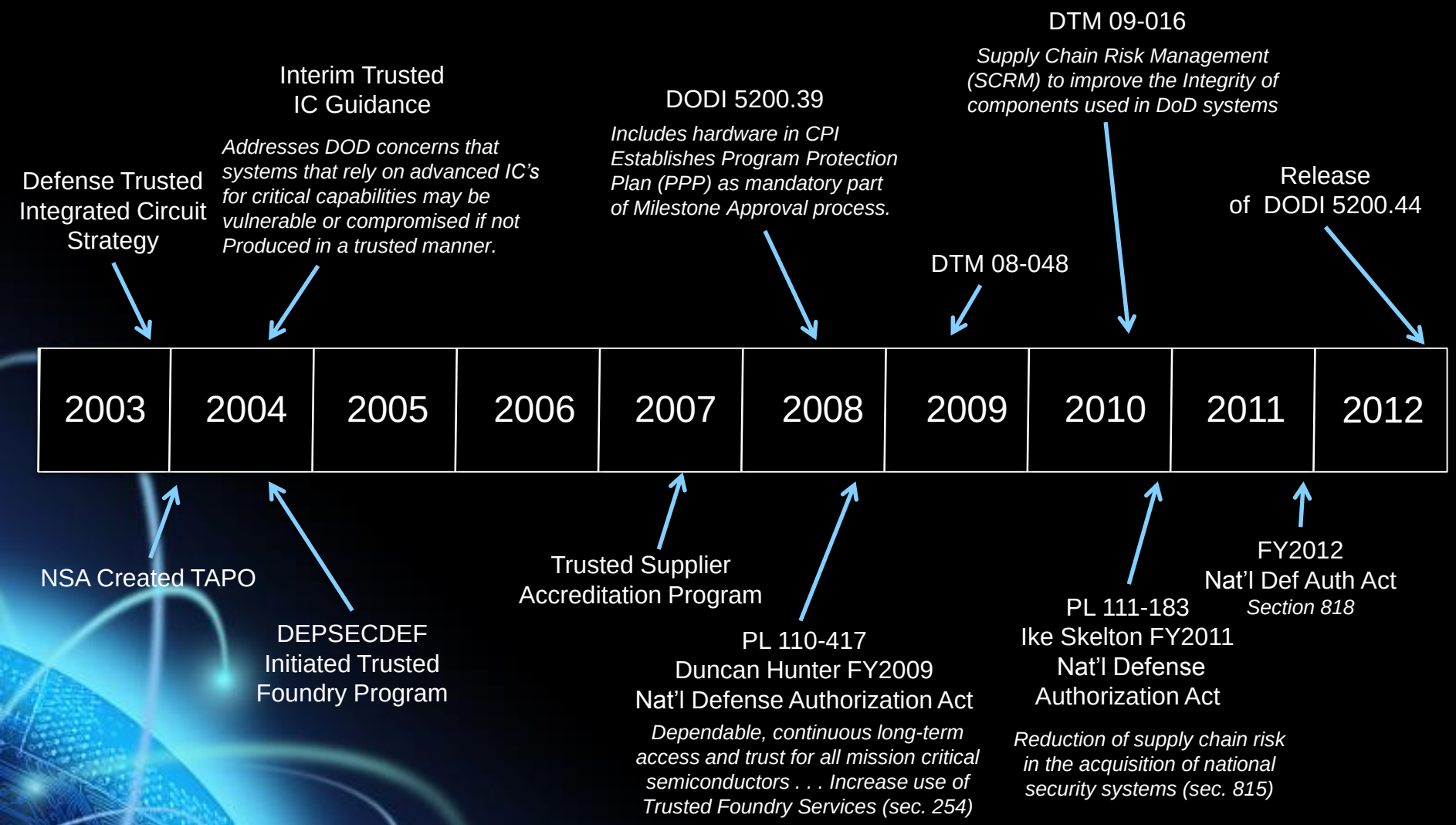
How to Obtain Trust

- Request trusted services via the designated point of contact at each supplier (POCs are on the accredited supplier list)
  - Ensures trusted flow will be employed
  - Ensures confidentiality of customer information

- <u>If a Trusted device is needed, Trusted services are required at each part of the supply chain</u>

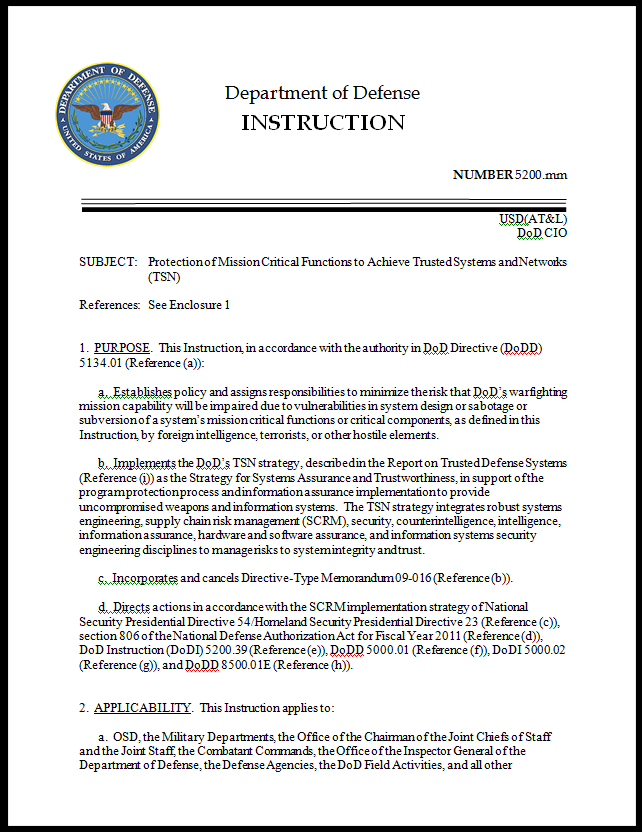
- A Trusted service (just like ITAR) is an option
  - Commercial (untrusted) services are also available at trusted suppliers
  - Trusted services are not automatic

Trusted IC Procurement Policy History



New Trusted Systems & Networks Policy

- DODI 5200.44 - Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)
- Implements what had previously been called Supply Chain Risk Management (DTM 09 016)
- What does it say about Microelectronics (Policy Section 4)?
  - C. Manage risk critical functions and components by"
    1. Reducing vulnerabilities
    2. Apply quality, configuration and security practices, with special attention to military end-use products and services
    3. Anti - Counterfeit Measures
    4. Rigorous Testing and Evaluation
    5. Tailored acquisition
    6. Use of IUID.
  - D. Document risk acceptance in the PPP
  - E. …Custom integrated circuit-related products and services shall be procured from a trusted supplier



Department of Defense
INSTRUCTION

NUMBER 5200.mm

USD(AT&L)
DoD CIO

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 authority in DoD Directive (DoDD) 5134.01 (Reference (a)):

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 (j)) as the Strategy for Systems Assurance and Trustworthiness, in support of the program protection process and information assurance 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 (b)).

d. Directs actions in accordance with the SCRM implementation strategy of National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (Reference (c)), section 806 of the National Defense Authorization Act for Fiscal Year 2011 (Reference (d)), DoD Instruction (DoDI) 5200.39 (Reference (e)), DoDD 5000.01 (Reference (f)), DoDI 5000.02 (Reference (g)), and DoDD 8500.01E (Reference (h)).

2. APPLICABILITY. This Instruction applies to:

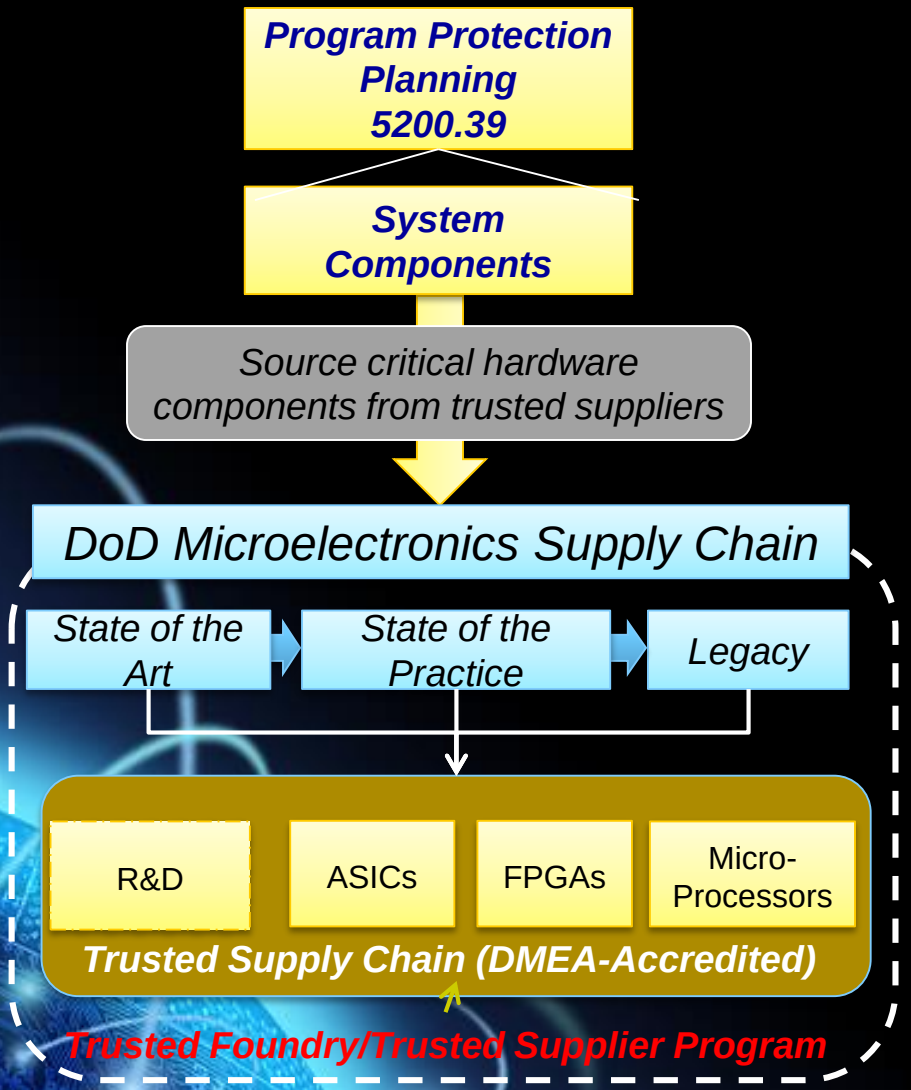
a. OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other

Signed on Nov 5th 2012

What 5200.44 Means To Programs

- Will need to assess and manage the supply chain risk for components in critical program information (CPI) and critical functions
  - Integrated Circuits
  - Field-Programmable Gate Arrays (FPGAs)
  - Printed Circuit Boards
- Will need to assess the risk from counterfeits to CPI and critical functions and develop a plan to mitigate and manage those risks
- Will need to identify Custom Design/Manufactured Integrated Circuits (ASICs) in CPI and critical functions and procured them through a Trusted supply chain

Supply Chain Risk Management



Program Protection Planning

- What: Mission-critical elements and components
- Who Identifies: System Engineers, Logisticians
- ID Process: Criticality Analysis
- Threat Assessment: DIA SCRM TAC
- Countermeasures: SCRM, SSE, Anti-counterfeits, software assurance, Trusted Suppliers, etc.
- Focus: "Keep malicious stuff out" by protecting key mission components

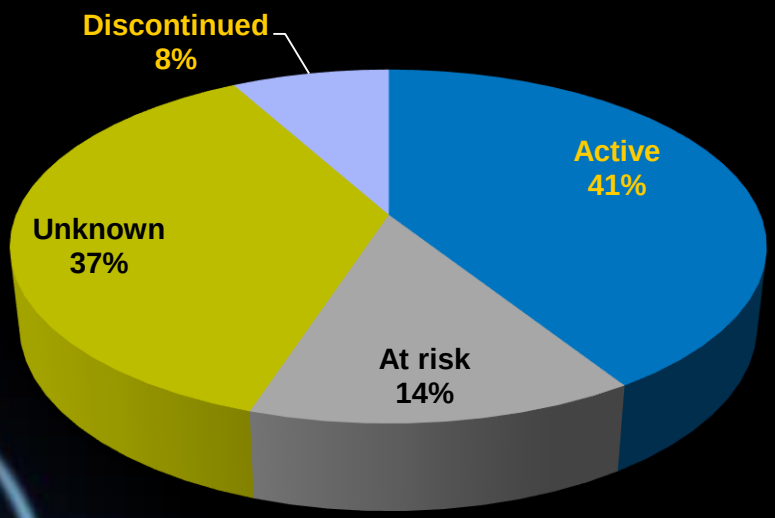
Protecting Warfighting Capability Throughout the Lifecycle

How will PPP affect Sustainment?

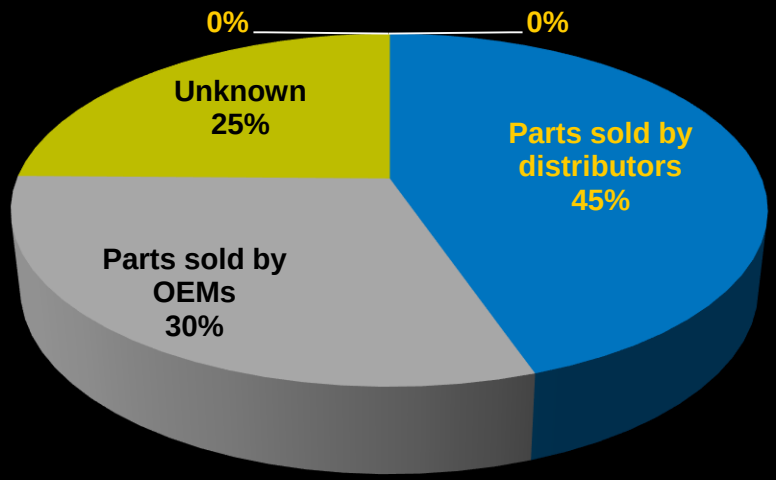
- Programs are identifying “Critical Components” which may invoke a range of mitigations
  - Sustainment will need to properly apply the program developed mitigations (testing, blind buys, ….)
  - Will changes to the risks during sustainment be coupled to PPP changes?
- The use of Trusted Suppliers will migrate to a requirement on sustainment
  - But Trusted Suppliers are not permanent, may fail, be acquired or leave the business . . . then what happens?
- How will “criticality” drive sustainment decisions
  - Will it be treated like safety critical?

Why is DMSMS an Acquisition PPP Issue?

**IC Use in 5 Major Systems Entering Production (Milestone C)*



Parts' Supply Phase



Parts' Supply Source

- Counterfeits pose a serious acquisition issue
- Key supply chain risks emerge in sustainment, but proper planning and mitigation must be done at acquisition

** A 2012 IDA study looked Bills of Material for 5 current major defense acquisitions, characterizing the use of over 3,000 unique ICs*

Summary

- Shifts towards a global industrial base and commercial products creates supply chain risks
- Problems like counterfeiting cannot just be assumed to be profit motivated criminal activities
  - Nation state counterfeiting can easily hide and be dangerously effective
  - Malicious intent concerns have not gone away
- After five years of growth, the Trusted supplier base has achieved major progress with more than 50 suppliers accredited
- New TSN policy requires programs to use Trusted microelectronics to protect critical program information through Program Protection Planning (PPP) across the life cycle of systems
  - DMSMS and sustainment issues play a role in PPPs and vice versa
  - The sustainment community has an important role in helping programs develop PPPs effective over the life cycle of systems

Conclusion

It is critically important that defense sustainment teams understand - - and take advantage of - - Trusted resources throughout program life cycle - - with initial component selection in the design and upgrade phases as well as with refurbishing activities where the threat of counterfeit components is the greatest.

- DMEA – DOD Program Management & Accreditation
  - (916) 231-1514
  - TrustedIC@dmea.osd.mil
- NSA – Trusted Access Program
  - https://www.tapoffice.org
- DBS (Outreach)
  - (202) 683-2021
  - cjortiz@definedbusiness.com