Trusted Foundry Program

Daniel M. Marrujo
Defense Microelectronics Activity
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
Trusted Integrated Circuit Supplier

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

Confidentiality

Integrity

Availability
Chronology

2003
- DEPSECDEF Memo
- Defense Trusted Integrated Circuit Strategy

2004
- Senator Lieberman Whitepaper
- USD(AT&L) Memos
  - Expansion of Trusted Foundry Program
  - Encouraging Industry Participation
  - Interim Guidance on Trusted Suppliers

2005
- DSB Task Force High Performance Microchip Supply
- DSB/MOD Task Force Defense Critical Technologies

2006
- DSB Task Force Mission Impact of Foreign Influence on DoD Software

2007
- Public Law 110-417 (Section 254)
- DMEA Trusted Supplier Accreditations Begin
- NSA/TAPO Desktop Accreditations

2008
- DoDI 5200.39 Critical Program Information
- DTM 08-048 Supply Chain Risk Management

2009
- Section 254 Report to Congress
- DoDI 5200.44 Critical Program Information

2010
- Program Protection Plan Outline & Guidance
- DTM 09-016 Supply Chain Risk Management

2011
- 2012
DoDI 5200.44
Trusted Systems and Networks

• Key Policy Objectives
  – Manage risk of mission-critical function and component compromise throughout lifecycle of key systems
    – Criticality Analysis is the systems engineering process for focusing activities
    – Mitigations: Supply chain risk management, software assurance, secure design
  – Use all-source intelligence analysis to inform procurement decisions
  – Codify trusted foundry requirement for DoD-unique ASICs
  – Document planning and accomplishments in PPP and IA Strategy

• Key OSD and Component Responsibilities
  – Advance state of the art in software assurance methodology and tools
  – Investigate “trust” implications for non-ASIC microelectronics
  – Analyze suspected and confirmed supply chain exploits across DoD

• Status
  – Formal coordination complete: No critical comments or non-concurs remain
  – Instruction signed November 5, 2012
Trusted Integrated Circuit Supply Chain

ISO 9001 Paradigm
Trusted Supplier Accreditation Process

DMEA
- Collect applicant data
- Assess basic eligibility
- Execution of CRADA and DD Form 254
- Cooperative Development of Technology Security Plan
- Achieve NISPOM compliance
- Facility Clearance Process (FOCI Adjudication, Personnel Security Clearances)
- Facility Clearance

Applicant Supplier
- Notification of interest / Request for information
- Review accreditation criteria
- Inspection and final documentation review
- Quality and/or Config. Mgt. Processes

DSS
- Issue Accreditation Certificate and Notices
54 Trusted Suppliers

As of 23 OCT 2012
# Trusted Foundry Technologies

As of 20 August 2012

<table>
<thead>
<tr>
<th>Trusted Foundry</th>
<th>CMOS</th>
<th>NVRAM CMOS</th>
<th>Mixed Signal CMOS</th>
<th>Mixed Signal CMOS+SONOS NVM</th>
<th>RF CMOS</th>
<th>HV CMOS</th>
<th>RH CMOS</th>
<th>RH CMOS+SONOS NVM</th>
<th>CMOS Image Sensors</th>
<th>Silicon Photonics</th>
<th>SOI CMOS</th>
<th>RH SOI CMOS</th>
<th>SOS</th>
<th>BiCMOS</th>
<th>Bipolar</th>
<th>GaAs</th>
<th>GaN</th>
<th>InP</th>
<th>SiGe</th>
</tr>
</thead>
<tbody>
<tr>
<td>BAE Systems Elettronica</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BAE Systems Microwave Electronics Center</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cypress Semiconductor</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mentor Graphics</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Honeywell Aerospace Plymouth</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MRL Laboratories, LLC</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IBM Corporation Burlington</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IBM Corporation East Fishkill</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Northrop Grumman Aerospace Systems</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Northrop Grumman Electronic Systems</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ON Semiconductor</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Oxford, Oregon</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ORI Semiconductor</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pacolet, Idaho</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ORI Semiconductor</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Raytheon RF Components</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sandia National Laboratories</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Stamina Semiconductor</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>STI Samoff</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TQnt Semiconductor</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Summary

- **Trusted Flow at Trusted Suppliers**
  - Provides an assured “Chain of Custody” for both classified and unclassified ICs
  - Ensures that there will not be any reasonable threats related to disruption of supply
  - Prevents intentional or unintentional modification or tampering of the ICs
  - Protects the ICs from unauthorized attempts at
    - Reverse engineering,
    - Exposure of functionality or
    - Evaluation of their possible vulnerabilities

- **Growing Participation**

- **Broad and Growing Technology Portfolio**

- **Trusted Integrated Circuit Supply Chain**
  - Mitigates IC Supply Chain Risk in Modern Commercial Environments
  - Simple to Utilize by Program Managers
  - No Inherent Schedule Impact vs. Commercial Flow – Practical for Fast-Turn Solutions
  - Small Additional Cost on Average
What’s in the Policy Memo?

– “Every acquisition program shall submit a PPP for Milestone Decision Authority review and approval at Milestone A and shall update the PPP at each subsequent milestone and the Full-Rate Production decision.”

– Expected business practice, effective immediately, and reflected in upcoming DoDI 5000.02 and DAG updates

– Signed by Principal Deputy, USD(AT&L) on July 18, 2011

The PPP is the Single Focal Point for All Security Activities on the Program

http://www.acq.osd.mil/se/pg/index.html#PPP
• Applies to all DoD critical information systems and weapons systems, which includes all major systems as defined by section 2302(5) of title 10, U.S.C.; national security systems as defined by section 3542 of title 44, U.S.C.; and all DoD information systems, categorized as Mission Assurance Category (MAC) I, and select DoD information systems, categorized as MAC II, in accordance with DoD Directive 8500.01E.

• It is DoD policy that supply chain risk shall be addressed early and across the entire system lifecycle through a defense-in-breadth approach to managing the risks to the integrity of ICT within covered systems.

• In part instituted with “processes to ensure that the fabrication of integrated circuits that are custom-designed and/or custom-manufactured (generally referred to as “application-specific integrated circuits”) for a specific DoD end use within covered systems are, as appropriate to the risk, performed by suppliers of integrated circuit-related services accredited through an authority designated by the USD(AT&L), unless expressly waived by the Milestone Decision Authority”
Growth in Available Services

As of 30 September 2012
Many Others In Work

As of 30 September 2012

- Broker: 7
- Design: 26
- Aggregation: 3
- Mask Mfg: 1
- Foundry Services: 18
- Post Processing: 5
- Packaging/Assembly: 20
- Test: 27

51 Suppliers
108 Services
Cost for Trusted Services

• Survey initiated in March 2012
• Purpose: Quantify the costs associated with obtaining trusted services
• Methodology: Requested from each supplier the added cost in % to obtain trusted services vs. untrusted (commercial) services from trusted suppliers
  – Average additional cost for Trusted Design Services: 9.1%
  – Average additional cost for Trusted Packaging/Assembly Services: 16.9%
  – Average additional cost for Trusted Foundry Services: 18%
  – Average additional cost for Trusted Test Services: 12.1%
How a Supplier Becomes Trusted

Candidate Supplier

Trusted Flow at Supplier

- Facility Clearance, FOCI adjudication/mitigation
- Cleared Chain of Custody
- Information System Security
- Configuration Management
- Quality
- Manufacturing Contingency Plan
- Scrap Controls
How to Obtain Trust

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

• **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

• **Trusted services are required at each part of the supply chain**
Website

http://www.dmea.osd.mil/trustedic.html

- Program Description

- Links to Official List of Accredited Suppliers
  - Company Name
  - Location
  - CAGE Code
  - Scope of Accreditation
  - Point of Contact
  - Email Address
  - Phone Number

- DMEA Trusted IC Accreditation Team
  - Phone Number
  - Email Address