


## **NDIA Trusted Microelectronics Joint Working Group**

### **Team 3: Trustable Microelectronics Standard Products**

Presented by  
Mr. Ken Lebo, Jacobs  
at NDIA's 8<sup>th</sup>  
Trusted Microelectronics Workshop  
February 2<sup>nd</sup>, 2017  
[kenneth.a.lebo.ctr@mail.mil](mailto:kenneth.a.lebo.ctr@mail.mil)

A solid red rectangular bar is positioned in the bottom left corner of the slide.

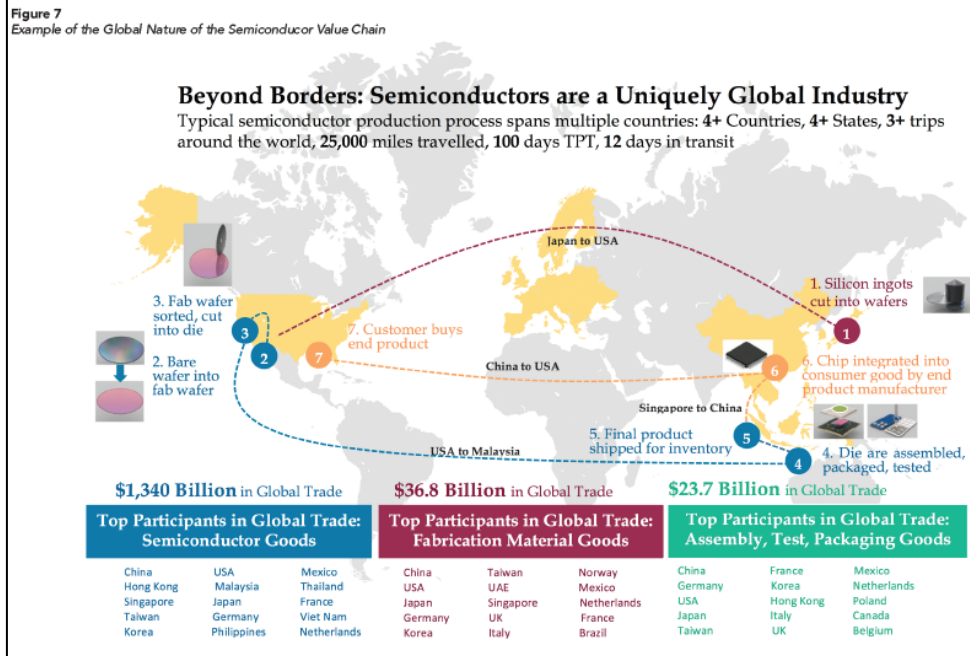
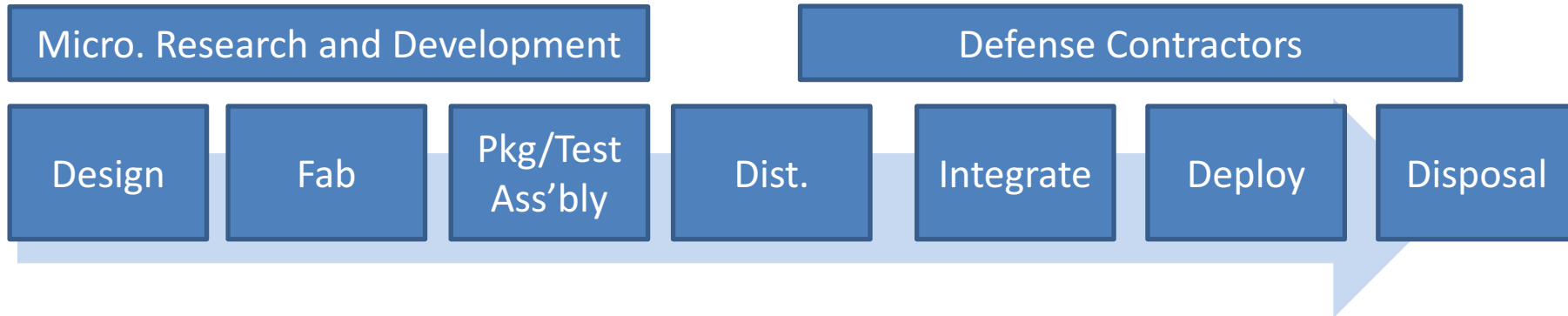
# Team Members

	Name	Organization
1	Bryan Brady	Avnet
2	Dean Brenner	Honeywell International
3	Edward Chatterly	Contract Support to ODASD(SE)
4	Saverio Fazzari	Booz Allen Hamilton
5	John Hallman	MacAulay-Brown, Inc.
6	Kenneth Heffner	Honeywell
7	Mike Holmes	Sandia National Labs
8	Ken Lebo (Team Leader)	Jacobs
9	Neal Levine	DMEA
10	Dave Meshel	The Aerospace Corporation
11	Greg Orne	Honeywell
12	Vashisht Sharma	Institute for Defense Analyses
13	Christopher Sims	NSWC Crane
14	Roger Van Art	Vantagepoint Advisors
15	David Weaver	SRI International

This team will consider these questions:

- *What are recommended methods for achieving confidence and assurance for a system or sub-system consisting of commercial microelectronics parts for DoD applications (DODI 5200.44) that are not manufactured using a DMEA Trusted flow?*
- *What are the effectiveness (assurance) and are the limitations (remaining risk) with the recommended methods?*
- *How much will it cost to implement these methods?*

# Commercial Components, Standard Products: A High Level View



**Business Models:**  
IDM  
Fabless/Foundry  
Variations – fab lite, etc  
In-source and Out-source

**Value Chain:**  
Design – IP, CAD  
Fab – tools, mat'ls, processes, yield, etc  
Pkg – internal and outsource  
Dist – interfaces to customers

- **This team will strive to leverage existing research and materials where possible.**
  - Interviews will be conducted with relevant industry subject matter experts (e.g., product integrity) to augment primary information from DoD Prime/Sub-Contractors and targeted adjacent industries to achieve product security/safety/quality.
- **The recommendations in the report will be based existing best practices and technologies without attempting to define processes or technologies that need to be developed.**

- **June – October 2016: First actions**
  - Revised the group's problem statement, obtained stakeholder buy-in and ownership of areas of further exploration (subgroups)
  - Planned first forays into adjacent industries for lessons learned, approaches, practices, etc.
  - Launched initial forays
- **October 2016: Team Lead (Dan Champion from Honeywell) moved to new career opportunity**
  - Sufficient support from team members to continue effort
  - New leader recruited and sharper focus developed
- **December 2016: Team restarts with initial focus on Trusted Supplier Framework summary**

# Adjacent Industry Forays

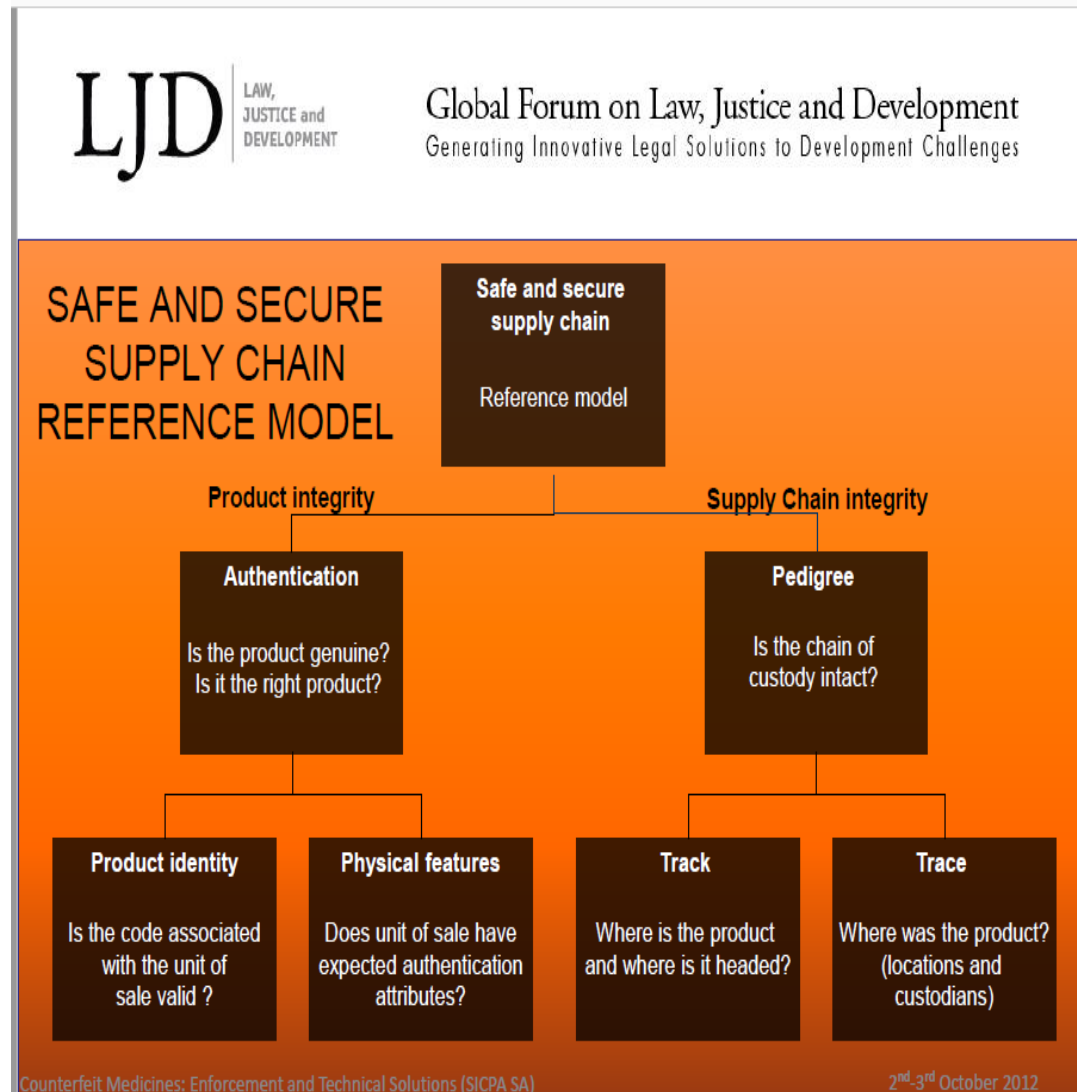
- Pharma
- Medical devices
- Food
- Automotive

## Parallels

- Supply chains
- Integrity of product
- Globalized

## Problems

- Gov't regulations vary
- Differences in technologies and implementations esp. w.r.t. chip fab



- **Buy from OEM or authorized franchise/distributor with Certificate of Conformance**
  - Supplier is qualified and has DLA QPL/QML implemented
- **If buying from a non-US entity (on-shore or off-shore)**
  - Company should require approval from a Government contracting officer, compliance with DFARs
  - CI review ( e.g. TAC Reports) for risk assessment
- **Should undergo robust screening, testing, and reverse engineering (may be small sample for critical parts)**
  - Use standard test for detection and mitigation: AS5553, AS6171, APR 6181 and other applicable ISO global standards and Open Source Accreditation Standards

*Team 3 started to look into adjacencies in other industries*

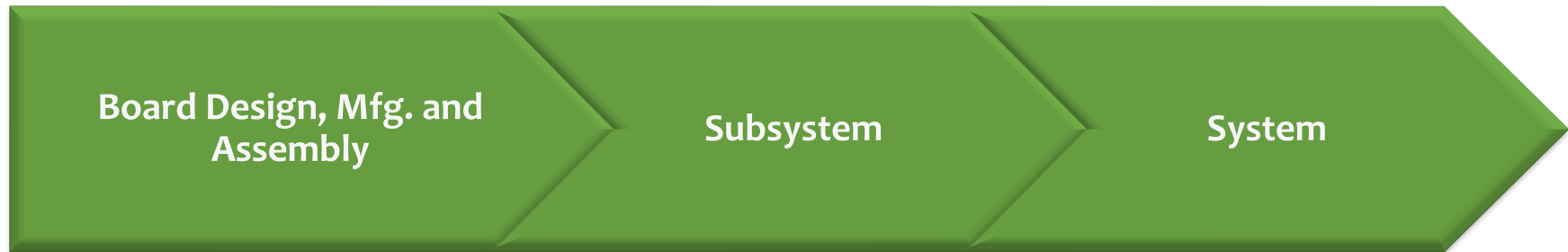


# New Approach: Separate Chip and Electronics Supply Chain Risks

## *Chip*



## *Supply Chain*



*Vulnerabilities:*

*Mitigations:*

Highly Simplified Representations

- Reached consensus to focus first on determining nominal “best practices” with respect to non-DMEA accredited microelectronics flows
- As a starting point, Team reviewed Trusted Supplier Framework (TSF) document that was put together by IDA and OSD / DMEA support contractors
- Team generated survey questions based on organization of the Framework
  - Consolidated team’s inputs into a single document
  - Identification process for industry people to send the survey
- **More recently, the team simplified the survey questions**
  - Distributed to industrial POCs; awaiting more responses

- **Based on NIST SP 800-161 as foundational organization of supply chain vulnerabilities**
- **Intended to help DoD buyers assess risks when purchasing electronic components outside traditional defense base**
  - TSF intended as a tool to help DoD buyers select appropriate supply chain risk mitigations when buying standard products
  - Focuses on actions a buyer can take to increase confidence in a supplier's trustworthiness
- **Provides a way for a DoD electronics component buyer to organize the landscape of existing standards and practices that mitigate supply chain risks . . .**
  - *Then allows the buyer to compare the mitigations and select those that best fit their program's risk and cost profiles*

# Areas Covered Under NIST 800-161 That Apply to HW Trustworthiness



- Access Control
- Audit and Accountability
- Configuration Management
- Contingency Planning
- Identification and Authorization
- Incident response
- Maintenance
- Physical and Environmental Protection
- Planning
- Provenance

*Team 3 members generated questions in these topical areas for a best practices request for info to be distributed to industry*

- *The NDIA Trusted Microelectronics Joint Working group is reviewing business practices, procedures, and industrial standards that can mitigate known and unknown risks in microelectronics design, fabrication and packaging for commercial applications.*
- *We invite you to submit the measures your company is practicing to protect your products, including those that are unique to your operations – such as the controls you describe to your customers to assure them of your product's integrity.*
- *Results will be used to develop standards and practices recommendations for improving guidance in acquisition of commercial integrated circuits for defense systems.*

## Companies Identified to Survey

- Analog Devices\*
  - Cirrus Logic
  - Cypress Semi\*
  - Dialog
  - GLOBALFOUNDRIES\*
  - IDT
  - Infineon
  - Intel\*
  - Honeywell\*
  - Jazz Semi (commercial)\*
  - Marvell
  - NXP
  - Maxim
  - Microchip\*
  - Micron\*
  - Micronas
  - Microsemi\*
  - NVIDIA
  - On Semi\*
  - Qorvo\*
  - Qualcomm
  - Renesas
  - Samsung
  - Semtech
  - Silicon Labs
  - Silicon Motion
  - Skyworks
  - SRI/Sarnoff\*
  - STMicro
  - Texas Instruments
  - Toshiba
  - Xilinx\*
- \* Contacted

# Several Survey Responses Received



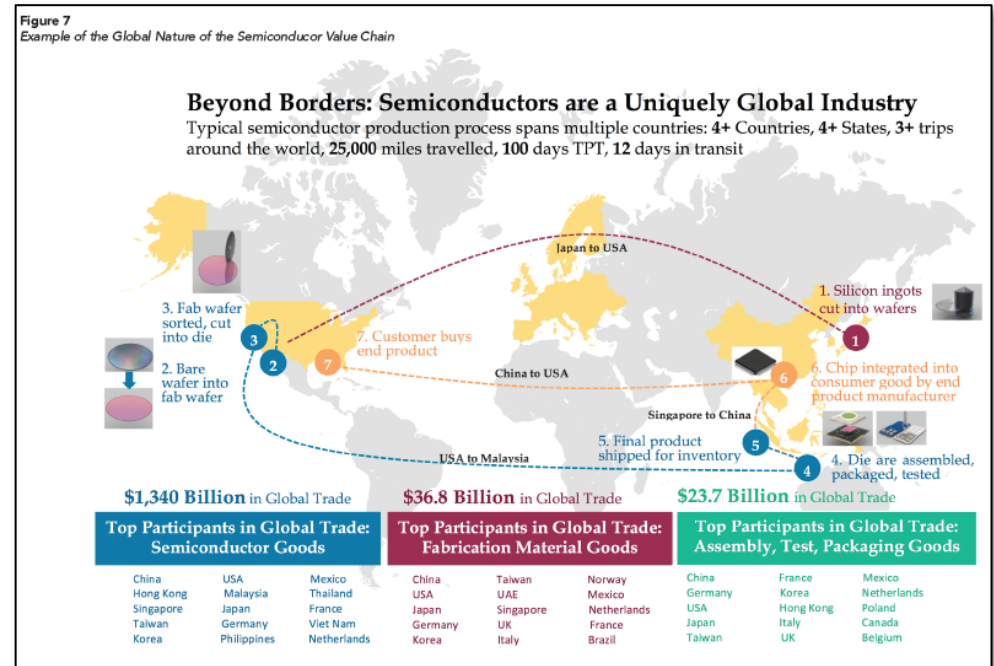
- **Detailed response from a large commercial semiconductor company**
  - Management of incoming supply chain
  - Defined development practices
  - Consistent worldwide manufacturing
  - Dependable enterprise infrastructure
  - Trusted outgoing supply chain
  - Global nature of supply chain
- **Inputs from DoD suppliers has confirmed instantiated practices of ITAR, Trust, and classification capabilities within DoD supplier base**

- **As secure as the weakest link...**
- **Ecosystem Threats and Mitigations**
  - Silicon
  - Supply chain
  - Programming
  - In the Field
- **Anti-counterfeiting measures**
- **Leveraging broad interests in enhancing security and IP**
- **Internal programs to address point problems**
  - trusted design center
  - Markings
  - Cooperation and participation



# A Word on Warranties...

- “No computer system can be absolutely secure.” (from a company’s response to our survey)
- Company makes no warranty with respect to any malfunctions or other errors in their hardware products or software products caused by virus, infection, worm, or similar malicious code not developed or introduced by company themselves.
- Company makes no warranty that any hardware products or software products will protect against all possible security threats, including intentional misconduct by third parties.
- Company claims they are not liable for any downtime or service interruption, for any lost or stolen data or systems, or for any other damages arising out of or relating to any such actions or intrusions.



## Next Steps for TM JWG Team 3



- **Press for more responses to survey and analysis**
- **Re-look at adjacent industries and business practices, government interactions**
- **Form a subgroup for more detailed 1-on-1 type interviews to probe further into commercial company practices that are basis of presumed trustworthiness in standard product components**
  - FPGA looks like an important standard product area to look at more carefully for practices and directions
- **Opportunity to contribute**
  - Seeking non-proprietary methods to secure products and supply chains
- **Goal to create collection of semiconductor and supply chain assurance methods and implementation paths to improve trustworthiness of commercial microelectronic components**