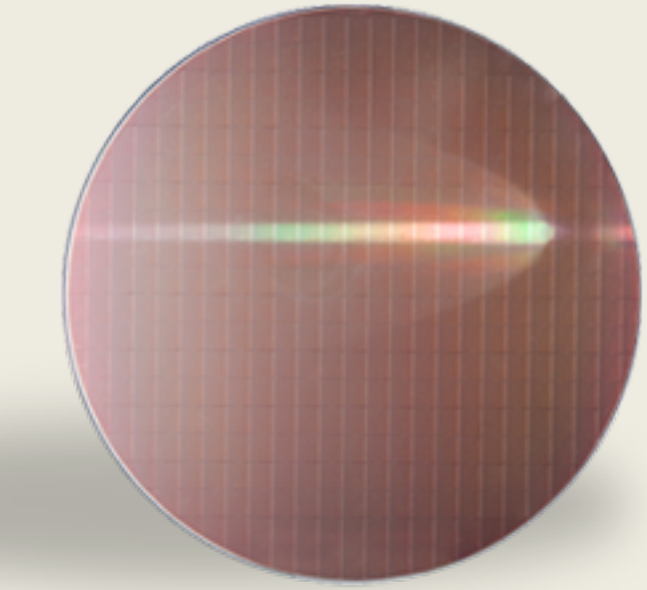
DMEA Trusted Foundry Program



NDTA-USTRANSCOM Fall Meeting

Microelectronics Risks Throughout the Defense Supply Chain

October 10, 2017

Catherine Ortiz

on behalf of the Trusted Foundry Program

Today's Discussion

Microelectronics background

Vulnerabilities: Globalization reduces visibility

Threats: Counterfeits and cyber attacks

DMEA Trusted Foundry Program

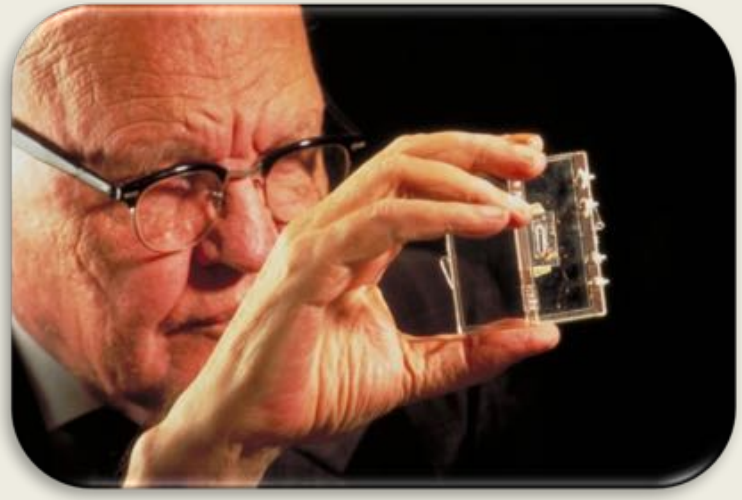
An assured supply chain: 78 Trusted Suppliers

Policy: Requirements for Trusted microelectronics

The future for Trust

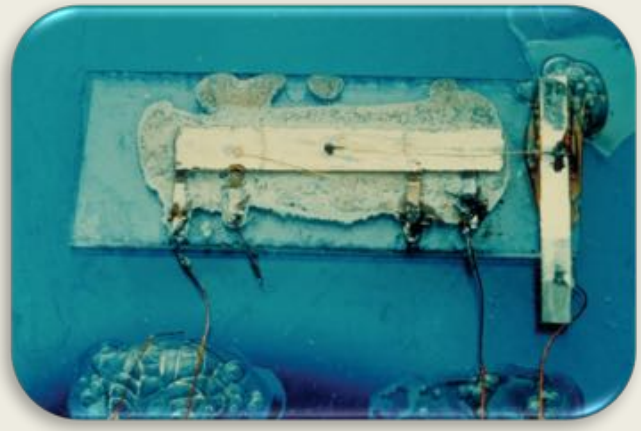
Microelectronics Background

Early Microelectronics



Nobel Laureate Jack Kilby at Texas Instruments

Kilby's original integrated circuit patented in 1959



Fairchild Semiconductor founders, 1960

Department of Defense and NASA were the primary research sponsors and key customers

Design and manufacturing by small, self-contained teams

Performance key focus

Security not a consideration

Microelectronics Provide Technology Advantage

Apollo Program
First Integrated Circuits
1960s

OH-58D Kiowa Warrior
Very High Speed Integrated Circuits
1980s

Microelectronics Provide Technology Advantage

F-22 Raptor
Digital Electronic Warfare
2000s

Block III Virginia Class Submarines
21st Century Electronics
2010s

Why Worry?

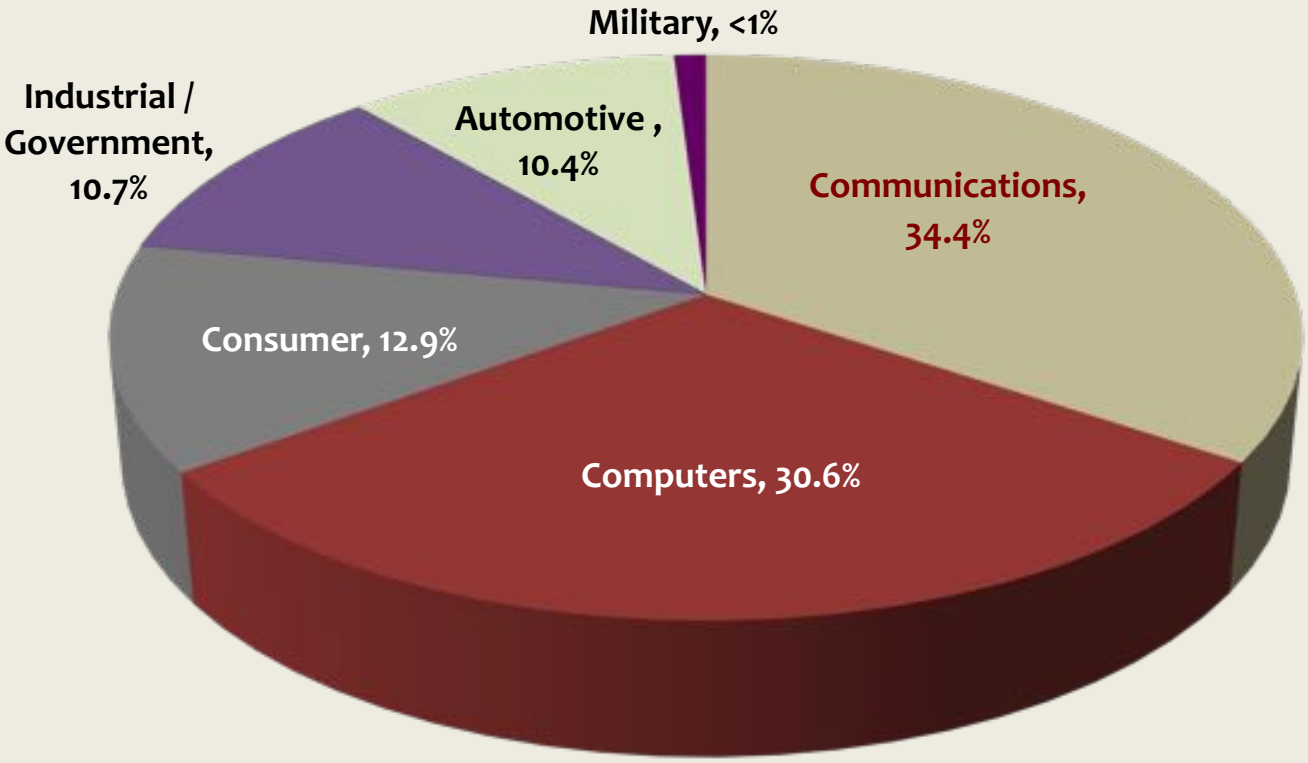
- Over the past decades the United States has built an increasingly sophisticated suite of defense and intelligence capabilities . . . in the process America has become a microelectronics junky
  - The application of technology has yielded incredible improvements in system performance . . . *but has simultaneously created a significant vulnerability by basing this performance on components that are susceptible to counterfeiting and tampering*
- Microelectronics purchasers encounter threats from both . . .

the demand domain in which program managers are far-removed from the component purchasing decisions and . . .

the supply domain in which the global semiconductor industrial capacity is increasingly found outside the U.S.

Vulnerabilities: Globalization Reduces Visibility

Today's Consumer Electronics Dwarf DoD Needs



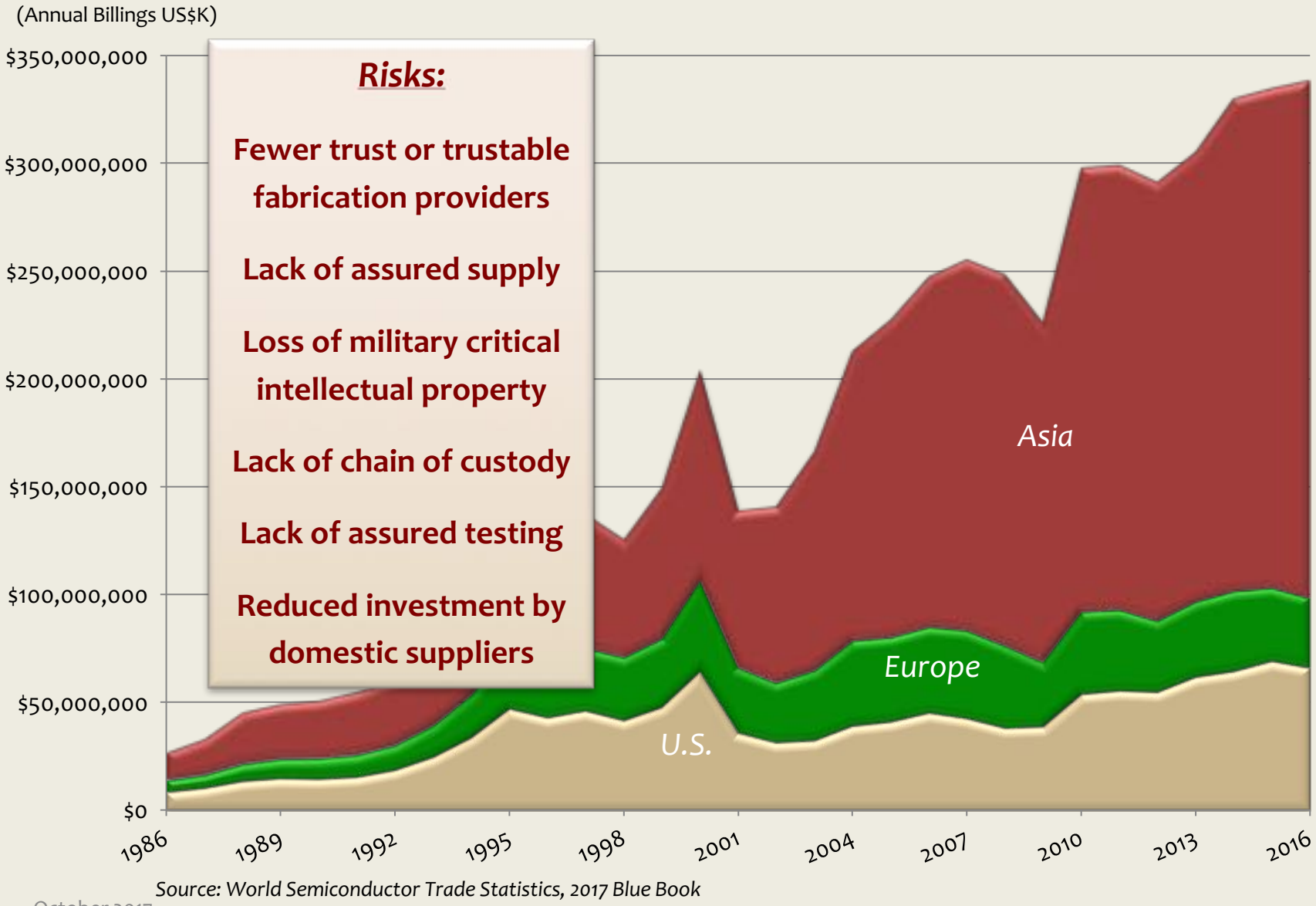
Risks:

Lack of ability to influence technology development

Loss of access to state-of-the-art technologies

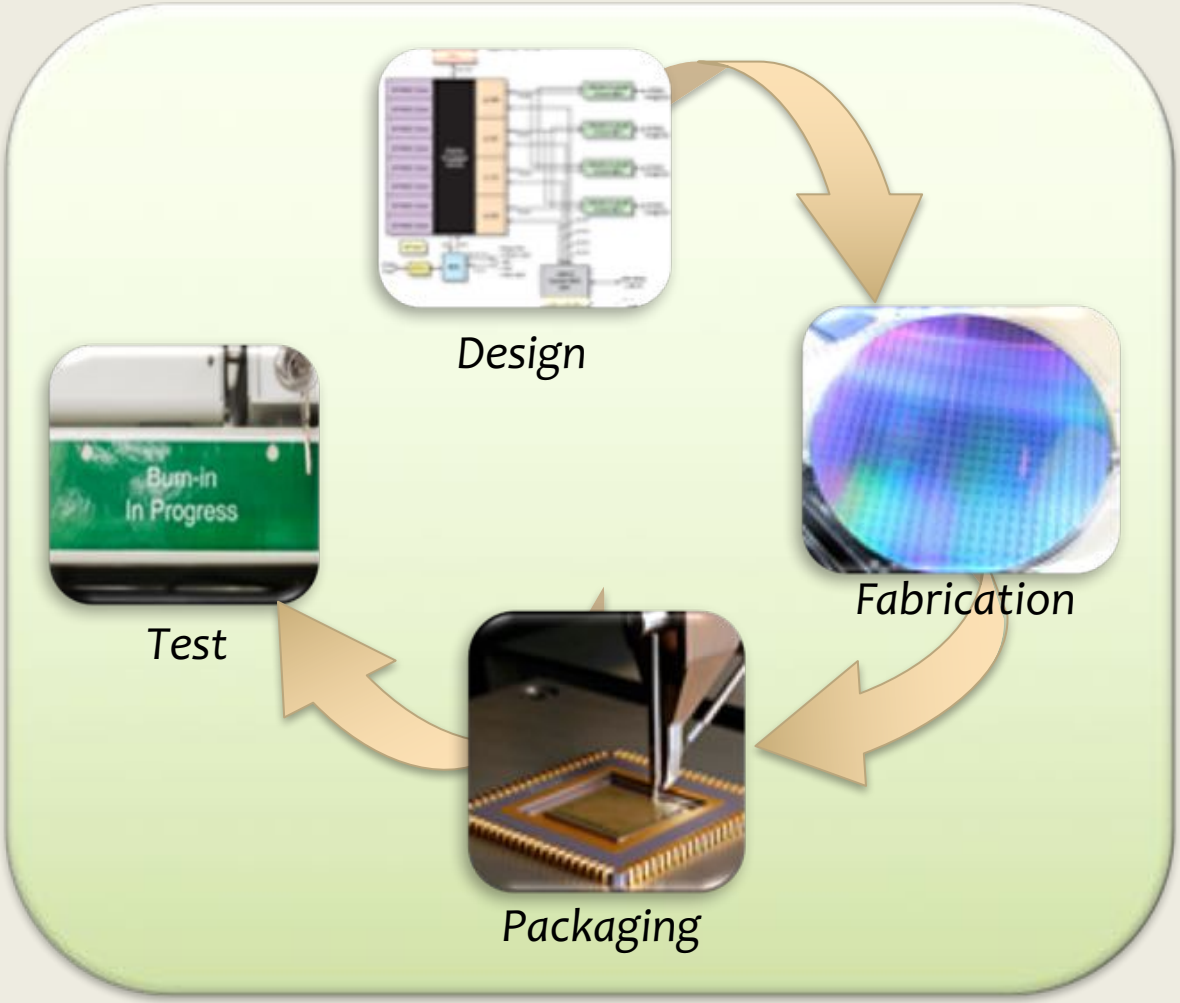
Source: World Semiconductor Trade Statistics (WSTS) and SIA Estimates

U.S. Fabs Are Not Keeping Pace with the Global Market



Source: World Semiconductor Trade Statistics, 2017 Blue Book

Multiple Threats in Semiconductor Production Cycle



Risks:

Lack of trustable designs

Lack of supply chain security

Tampering potential

Reverse engineering and IP siphoning

Lack of chain of custody

Unauthorized copies

Remarking and counterfeiting

Scrap diversion

World's 300mm Capacity and Location

IDA

Total World Capacity (wafers/mo) and Location - 300mm

EUROPE / MIDDLE EAST – 270,155
* CEA-Leti - 3,000
* GlobalFoundries - 80,000
• Infineon - 30,000
• *Infinion- 3,000
• Infineon/CNT - 3,000
* Intel(Ireland) - 70,000
+ Intel(Israel) - 60,000
* STMicroelectronics – 15,155
* imec - 6,000

CHINA – 517,800
* Global Foundries – 10,000
* Intel - 30,000
~ Powerchip (JV Hefei) - 40,000
• SK Hynix - 150,000
* SMIC - 52,000
• SMIC - 15,000
• SMIC/Beijing government JV – 19,800
* Samsung - 50,000
* Shanghai Huali Microelectronics - 35,000
@ Shanghai Huali Microelectronics - TBD
*TSMC - 0
*UMC 50,000
*YRST/ XMC - 60,000

KOREA – 1,432,000
* Alchimer S.A. - TBD
* SK Hynix -535,000
* Samsung - 897,000

JAPAN – 952,400
* Fujitsu - 45,000
* Micron (Elpida) - 130,000
* ROHM - 20,000
* Renesas - 16,000
* Sony – 115,000
* Toshiba – 6,400
* Toshiba/SanDisk 610,000
* TowerJazz –10,000

UNITED STATES – 637,125
+ American MiniFoundry - TBD
* CNSE Albany - 10,000
* GlobalFoundries - 65,000
* GlobalFoundries (was IBM) - 14,000
• IM Flash Technologies (JVIntel-Micron) - 48,000
* Intel - 225,000
* Micron Technology - 95,000
* NOEL Technologies - TBD
* Novati Technologies (Tezzaron Semiconductor) - 5,000
* Samsung - 80,000
* Texas Instruments – 95,125
~ ams/NY state - 0

TAIWAN – 1,514,000
* Macronix - 20,000
* Micron – 215,000
* Nanya Technology - 60,000
* Powerchip -100,000
* TSMC – 928,000
* UMC – 120,000
* Winbond – 71,000

ABU DHABI – 0
~ GlobalFoundries /ATIC – 0

SINGAPORE – 333,440
* GlobalFoundries – 83,333
* Institute of Microelectronics (IME) - TBD
• Micron Technology – 65,000
• * Micron/Flash – 140,000
* UMC – 45107

(*) Operating Fabs
(+) Fabs under development
(~) Announced Fabs
@ On Hold

300 mm 2017 World Operating Capacity = 5,656,920 w/mo

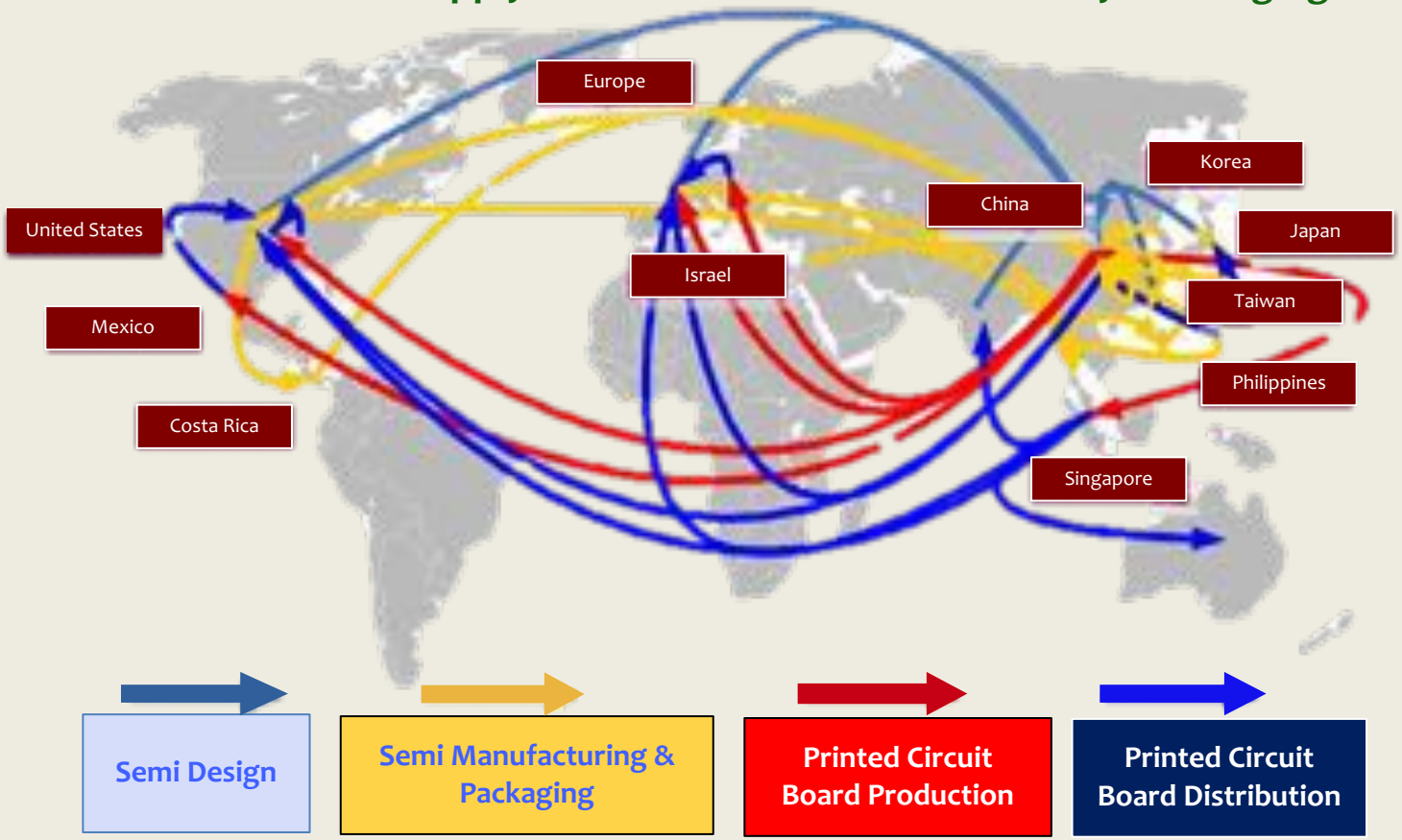
Most of the world's accessible and leading-edge capacity is in Asia

Semico Fab Database 2017

DISTRIBUTION STATEMENT C. Distribution authorized to U.S. Government Agencies and their contractors. Other requests shall be referred to DMEA.

Defense Supply Chains Are Becoming More Complex

Global nature of supply chains make the chain-of-custody challenging

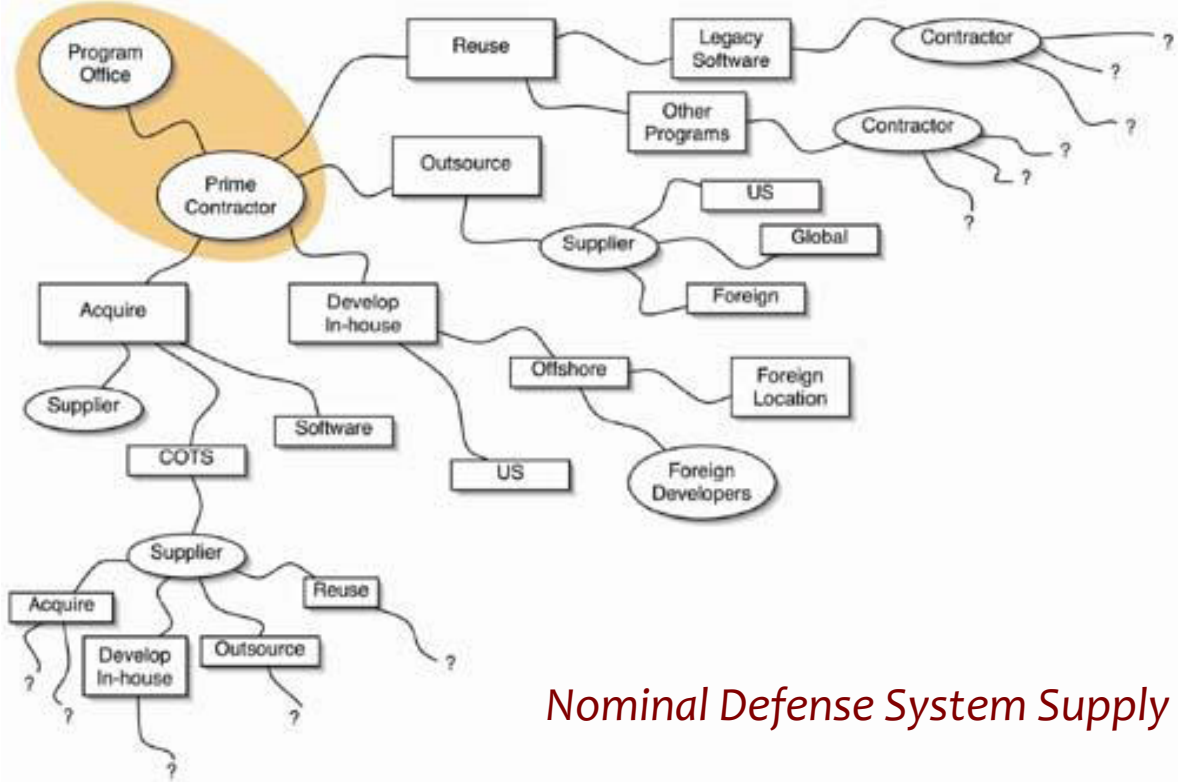


Source: IDC Manufacturing Insights & Booz Allen analysis

Lifecycle shown for a single Joint Strike Fighter component

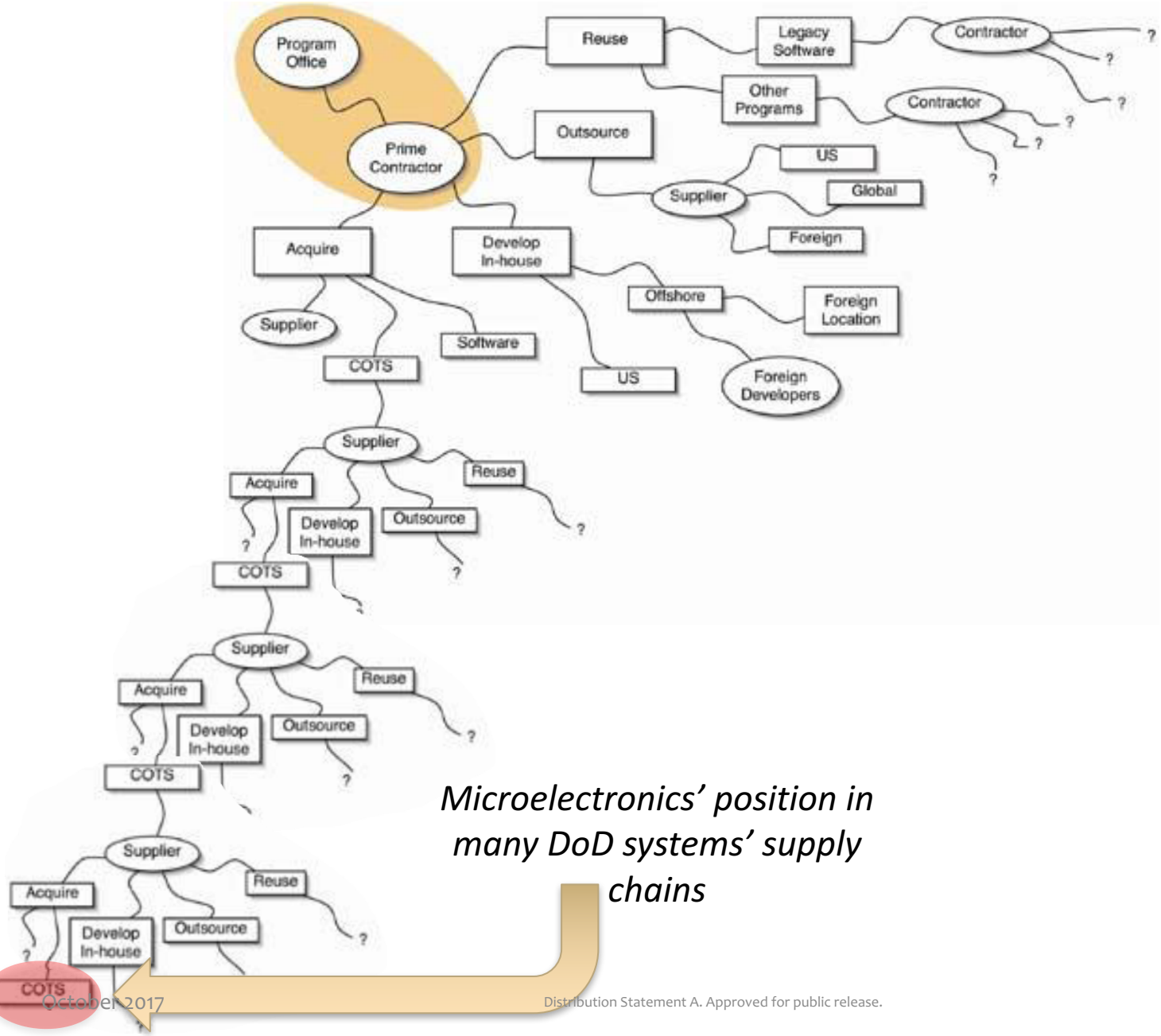
-Component changes hands 15 times before final install

Slide Source: DARPA Microsystems Technology Office--Approved for Public Release

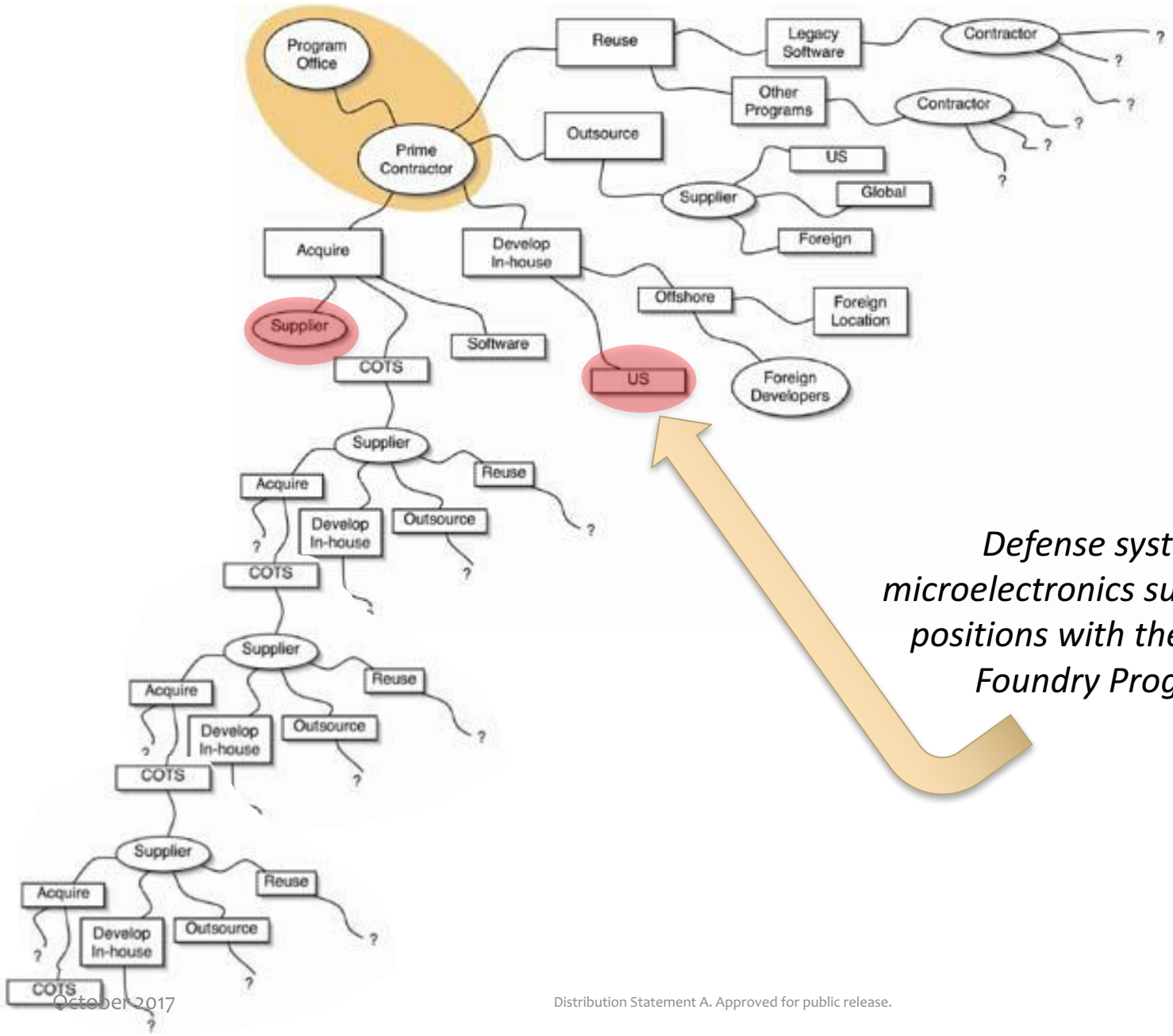


Nominal Defense System Supply Chain

Sources: "Scope of Supplier Expansion and Foreign Involvement" graphic in DACS www.softwaretechnews.com Secure Software Engineering, July 2005 article "Software Development Security: A Risk Management Perspective" synopsis of May 2004 GAO-04-678 report "Defense Acquisition: Knowledge of Software Suppliers Needed to Manage Risks"



Microelectronics' position in many DoD systems' supply chains



Defense systems microelectronics supply chain positions with the Trusted Foundry Program

Threats: Counterfeits and Cyber Attacks

Vulnerabilities from Counterfeit Chips

BusinessWeek (Oct 2, 2008) article entitled "Dangerous Fakes" reports on recycled and counterfeit military chips from China-based suppliers entering DoD supply chain.

E2-C Hawkeye

Chip used in navigational system

F-15 Fighter

Chip used in flight control system

Parts Unknown: Examples where counterfeit parts found….DATA: BW Research, DLA

Source and Ref's: http://www.bloomberg.com/news/articles/2008-10-01/dangerous-fakes

Cybersecurity Hardware Vulnerabilities

"The risk of compromise in the manufacturing process is very real and is perhaps the least understood cyberthreat . . .

Tampering is almost impossible to detect and even harder to eradicate . . .

Remotely operated 'kill switches' and hidden 'backdoors' can be written into the computer chips . . .

allowing outside actors to manipulate the systems from afar."

-- Deputy Secretary of Defense William Lynn III

http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain


FOREIGN AFFAIRS

SEPTEMBER/OCTOBER 2010

Defending a New Domain

The Pentagon's Cyberstrategy

William J. Lynn III

Much of early cybersecurity discussion focused on threats from software and process vulnerabilities . . . the semiconductors may present even greater risks

German Missiles "Hacked By Foreign Source"

A German missile system stationed on the Turkish-Syrian border was reportedly hacked by a "foreign source" and carried out "unexplained commands".

The report by German civil service magazine *Behörden Spiegel* does not give details about what these orders were or when they were carried out, ***but suggests hackers may have gained access to the missile system through a computer chip which guides the missiles***, or through a real-time information exchange which allows the missiles to communicate with their control system.

Germany's President Joachim Gauck and his partner Daniela Schadt listen to commander of German troops in Turkey Colonel Stefan Drexter as they visit Patriot missile batteries in Kahramanmaras April 27, 2014.Osman Orsal/Reuters

Newsweek, July 8, 2015

Ewan Lawson, a cybersecurity expert at defense think tank Royal United Services Institute for Defence and Security Studies, says that hacks of military missile systems may be more common than realized but go unreported for security reasons; and that only nation-states would have the capacity to hack such a system.

Cyber Espionage: Operation Bugdrop

Operation Bugdrop, a new, large-scale cyber-reconnaissance operation targeting a broad range of targets in the Ukraine. It eavesdrops on sensitive conversations by remotely controlling PC microphones – in order to surreptitiously "bug" its targets – and uses Dropbox to store exfiltrated data.

At least 70 victims were targeted by the operation in a range of sectors including critical infrastructure, media, and scientific research.

Most of the targets are located in the Ukraine, but there are also targets in Russia and a smaller number of targets in Saudi Arabia and Austria.

Hackers siphoned 600GB of voice and entered data by taking control of PC microphones

DMEA Trusted Foundry Program

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
  - In October 2014, IBM announced its plans to transfer its microelectronics fabrication capability to GLOBALFOUNDRIES . . . more on this later . . .
- 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, 78 suppliers are accredited to provide services ranging from design - - fab - - mask manufacturing - - packaging & testing

Trusted Foundry Program Created to Mitigate Risks

- The Trusted Foundry Program (TFP) was established in 2003 as a joint effort between DoD and National Security Agency

Trusted Foundry Program continues to evolve to meet today's defense microelectronics needs . . .

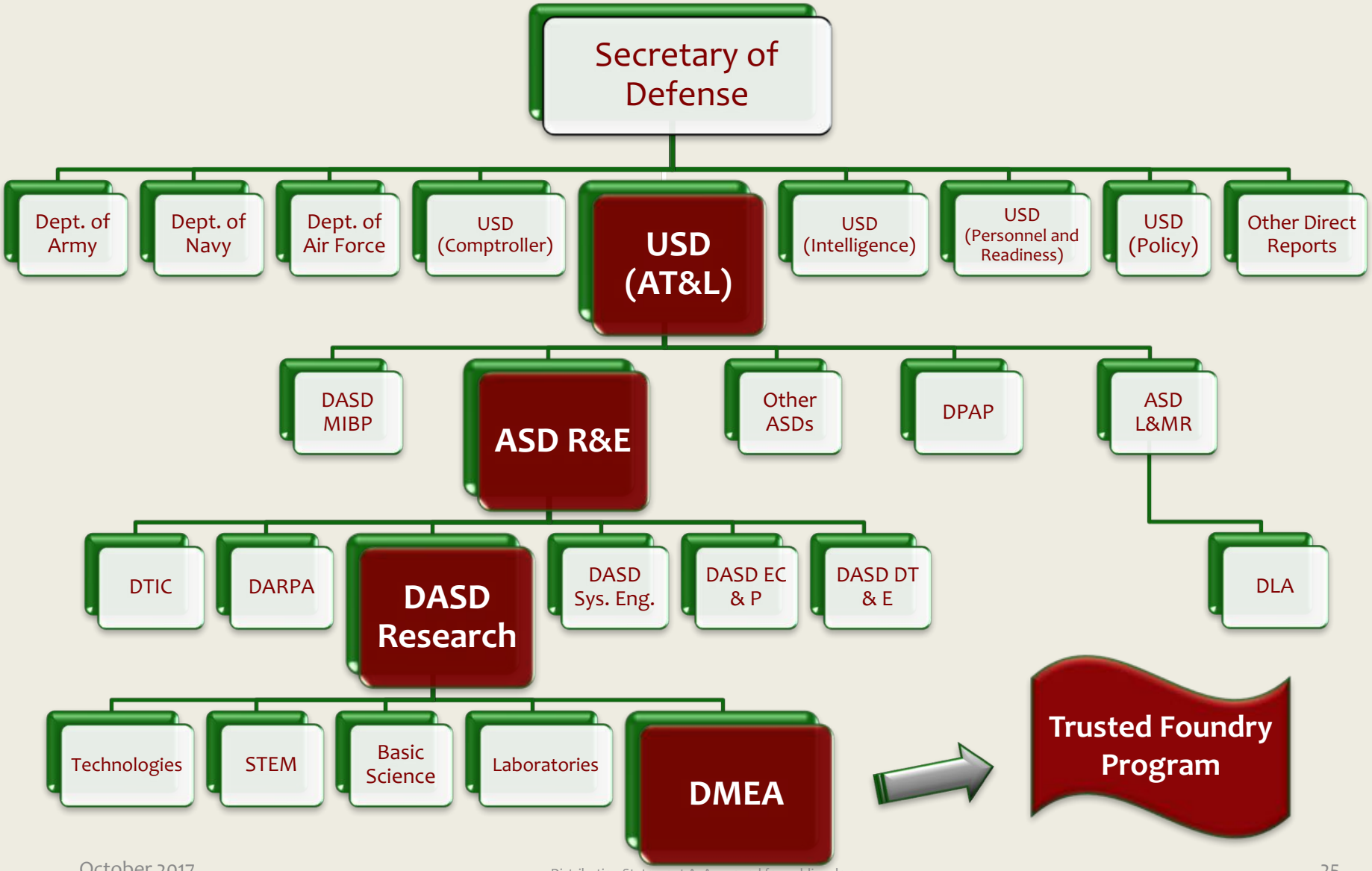
- Trusted Foundry Access 2 (TFA2) contract awarded by DMEA in April 2016 with overall period of performance through March 2023
  - ASIC and foundry services
  - Pricing based on aggregated demand
  - Commercial, ITAR, and Trusted flows for all commercially available technologies from GFUS2
  - Facilitates advanced access to other leading edge semiconductor technologies (case-by-case)
    - e.g. Fab 8 14LPP GlobalShuttle
  - Enterprise licenses for common design IP

Fab 9 (Burlington, VT)

Fab 10 (East Fishkill, NY)

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

The Trusted Foundry Program in OSD



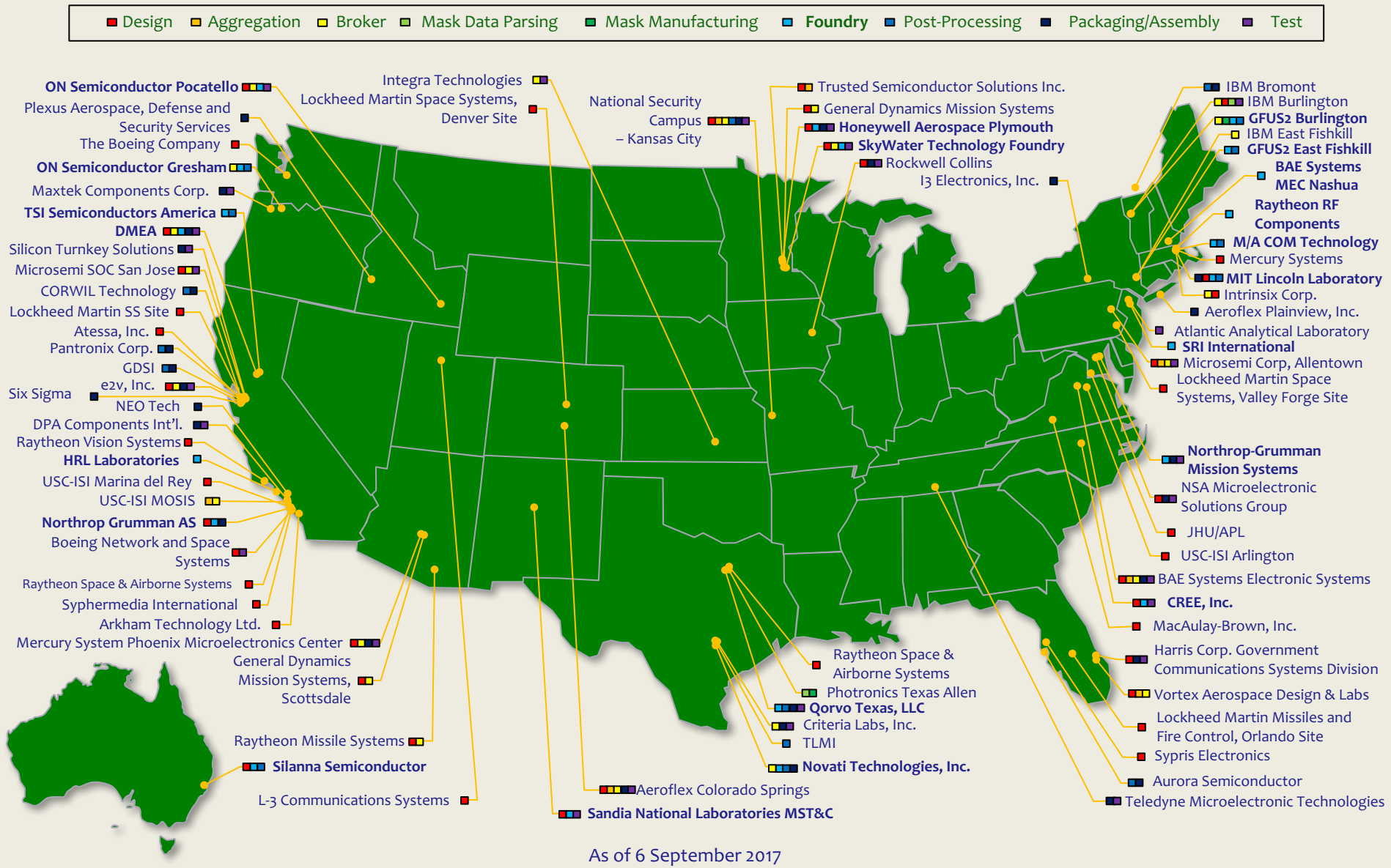
Trusted Defense Systems Strategy

Drivers/Enablers

- National cybersecurity strategies
- Congressional interest
- DoD policy and directives
- Globalization challenges
- Increasing system complexity

An Assured Supply Chain: 78 Trusted Suppliers

78 Trusted Suppliers



As of 6 September 2017

System Level Trust Concerns

	ASIC/ASSP	*MOTS Microprocessors, DSPs, etc.*	*FPGAs / Programmable SOCs*	*Low complexity standard parts*
Tampering	✓	✓	✓	
Counterfeits		✓	✓	✓
Unauthorized Overproduction	✓	✓	✓	
Supply Chain CPI Confidentiality	✓			
Programmed CPI Confidentiality			✓	
Foundry Availability & Access	✓	✓		

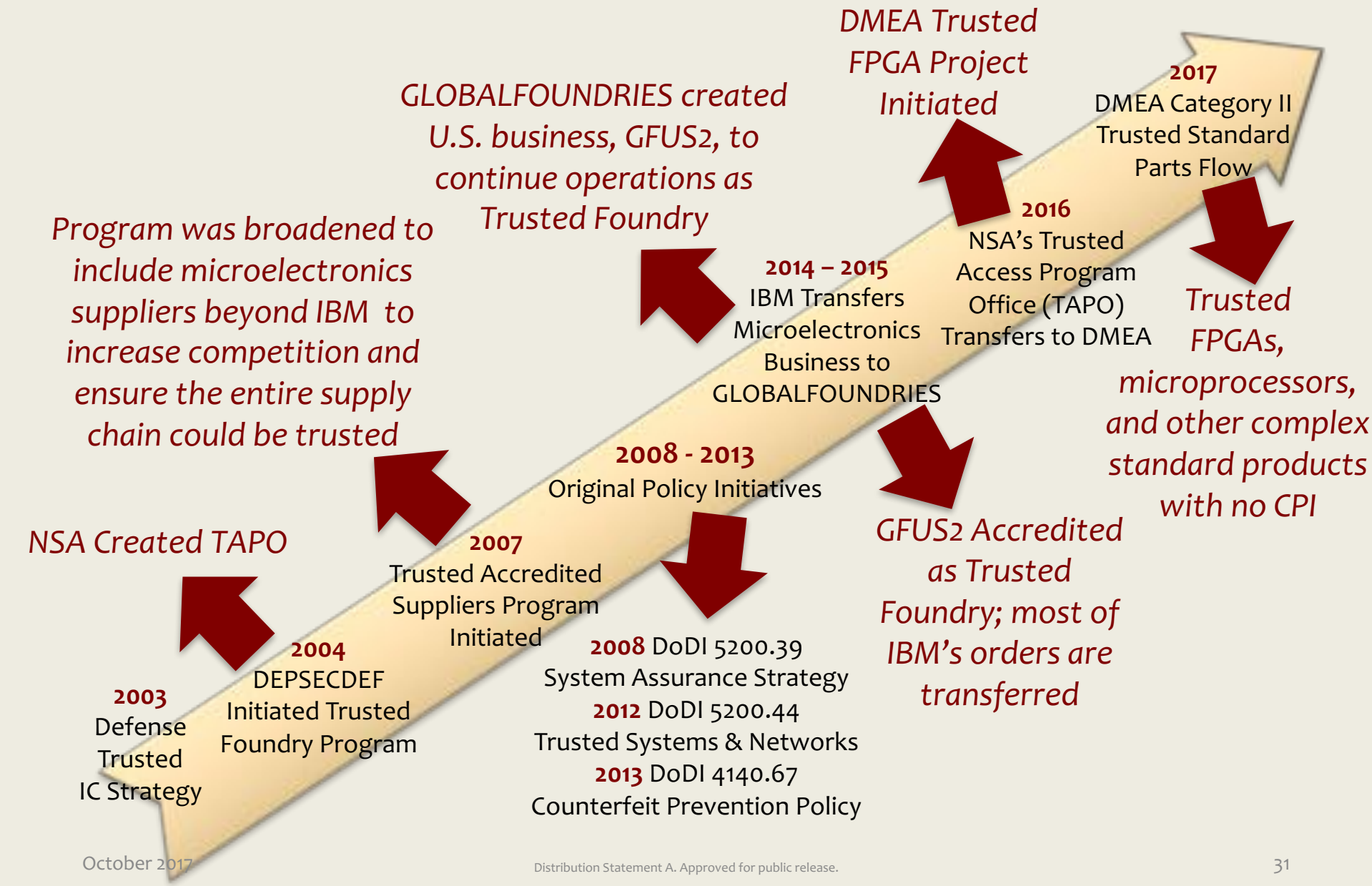
Trust is Multi-Dimensional; Concerns are Component Dependent

Trusted Suppliers 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
- **Category II Trusted Standard Parts & FPGAs**
- 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
- Post-processing, such as wafer bumping

78 Accredited Trusted Suppliers are available for a full range of microelectronics design, production, and test for leading-edge, state-of-the-practice, & legacy microelectronics

Trusted Foundry Program Timeline



Long-Term Strategy Time Line

DoD Trusted Foundry Program Consolidation - Defense Microelectronics Activity (DMEA)

Transition

Newly Established Trusted Foundry Contract

Sustained Network of Trusted Certified Suppliers

Trusted and Assured Microelectronics Program:

Alternate Source for Trusted Photomasks

Preparation activities

Capability Development

Deploy new capability

Verification and Validation (V&V) Capabilities and Standards for Trust

Preparation activities

Improve capabilities and capacity, and provide support to program needs, for analysis of microelectronics trust

Identify and develop standards, practices, and partnerships to improve availability of trust from commercial providers

Advanced Technology and Alternative Techniques for Microelectronics Hardware Trust

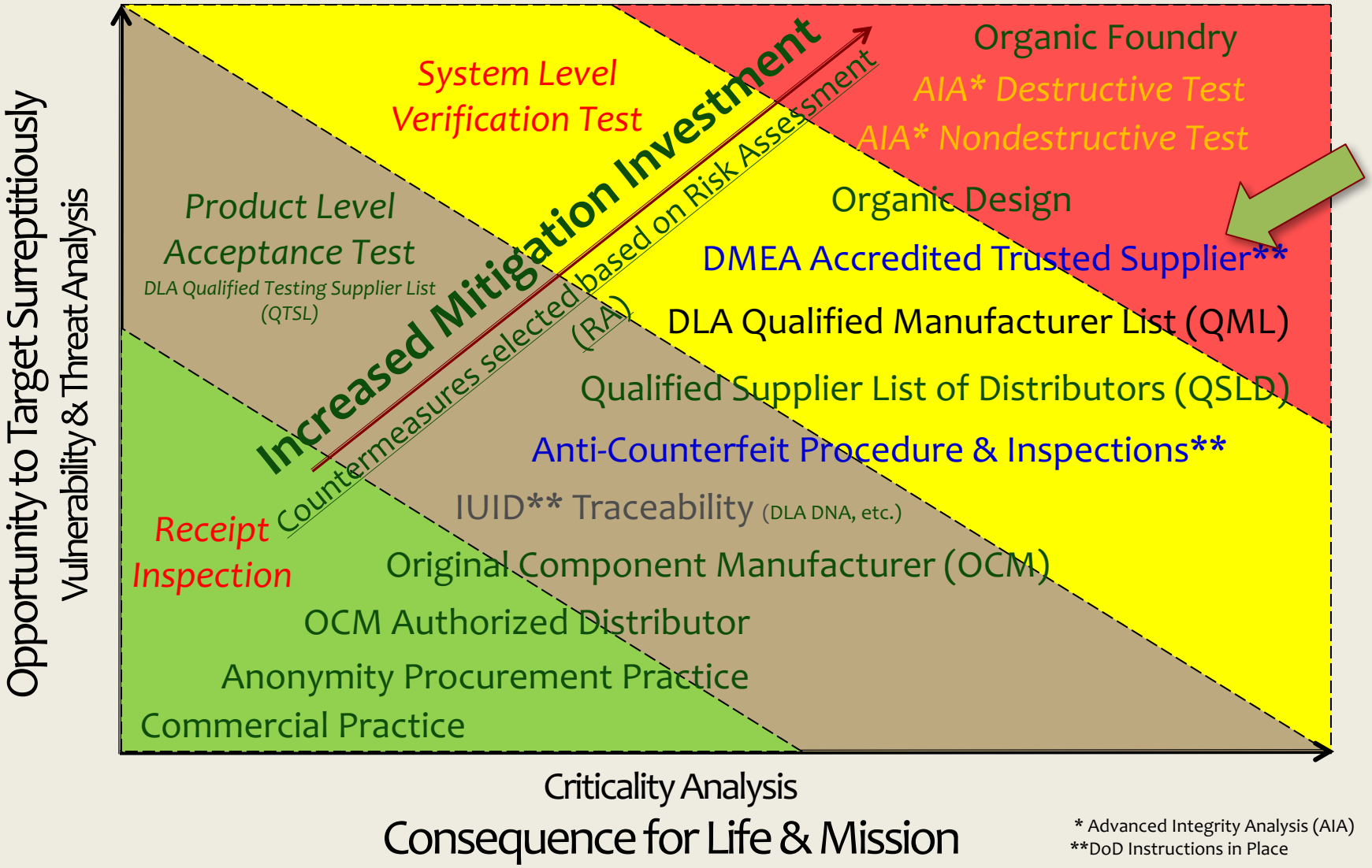
Preparation activities

Capability development and demonstration

Deploy new capabilities

2015 2016 2017 2018 2019 2020 2021 2022 2023 2024

Supply Chain Risk Countermeasures



* Advanced Integrity Analysis (AIA)
**DoD Instructions in Place

Trust Accreditation and DLA Programs

- Defense Logistics Agency programs are focused on quality
  - Qualified Parts List (QPL) – a process that qualifies that products meet a specification
  - Qualified Manufacturers List (QML) – assures that the supplier uses an approved quality system
  - QSLD (Qualified Suppliers List of Distributors) – assures that distributor not only maintains quality system, but also practices to ensure authenticity
- Trusted Supplier accreditation is focused on security
  - Requires DSS SECRET facility clearance and SECRET clearances for all personnel handling product or ICT connected to product's manufacturing
- DLA programs and Trusted Supplier accreditation both qualify "trustworthy" suppliers, using different criteria . . . but the Trust accreditation is required for some military-specific components

DMEA TFP FY2018 Goals – from President's Budget Request

- Continue facilitating the availability of Trusted state-of-the-art semiconductor technology to DoD weapon system programs and research organizations through the DMEA Trusted Access Program office contracts.
- Enhance the cadre of trusted suppliers for the critical trusted components and services needed for appropriate defense systems.
- Enhance Trusted Microelectronics products to include newly available leading edge technologies and other key specialty processes required by Department programs.
- Expand a line of trusted catalog components that can be purchased by Defense contractors.
- Continue activities that ensure the DoD has Trusted Access to leading edge semiconductor technologies.
- Continue the development of a capability for the inspection and analysis of application-specific integrated circuits (ASICs) and continuously refine the utilized methods for efficiency, accuracy, and applicability to multiple processes.

Summary

- Access to microelectronics technology is critical for military advantage
- ***Shifts towards a global industrial base and commercial products creates access and supply chain security risks***
- Comprehensive cybersecurity must address hardware risks as well as software and process vulnerabilities
- The Trusted Accredited Suppliers provide a deep portfolio of products and services with 78 suppliers accredited
- Broad recognition of the need for new approaches to retain trustable, leading-edge capabilities

Trusted Foundry Program Continues to Evolve to Meet Today's Government Microelectronics Requirements

Conclusion

It is critically important that the defense programs understand - - and take advantage of - - Trusted resources throughout program lifecycle - - 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.

DoD Resources

- DoDI 4140.67 DoD Counterfeit Prevention Policy (April 2013)
  http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/414067p.pdf
- DoDI 5000.02, Change 3, Operation of the Defense Acquisition System (August 2017)
  http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500002_dodi_2015.pdf
- DoDI 5200.39 Critical Program Information (CPI) Identification and Protection Within Research, Development, Test, and Evaluation (RDT&E) (May 2015)
  http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/520039p.pdf
- DoDI 5200.44, Change 2, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN) (July 2017)
  http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/520044p.pdf
- Policy Memorandum (PM) 15-001 – Joint Federated Assurance Center (JFAC) Charter (February 2015)
  http://www.acq.osd.mil/se/docs/JFAC-Charter-Signed-9Feb2015.pdf
- DoDD 5200.47E Anti Tamper (AT) Change 1 (August 2017)
  http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/520047E.pdf
- Department of Defense Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs (January 2017)
  http://www.acq.osd.mil/se/docs/2017-RIO.pdf
- Defense Acquisition Guidebook (DAG), Chapter 9 Program Protection (February 2017)
  https://www.dau.mil/guidebooks/Shared%20Documents/Chapter%209%20Program%20Protection.pdf
- DoD Systems Engineering Initiatives (July 2017)
  http://www.acq.osd.mil/se/initiatives/init_pp-sse.html

- DMEA – DOD Program Management & Accreditation

  (916) 568-4057

  tapo@dmea.osd.mil

- DBS – Outreach (contractor)

  (202) 683-2021

  cjortiz@definedbusiness.com