Building Hardware Assurance with Trusted Suppliers: Creating Multi-layered Security

Systems and Mission Engineering Conference 2022

November 2, 2022

Dave Chesebrough

Defined Business Solutions

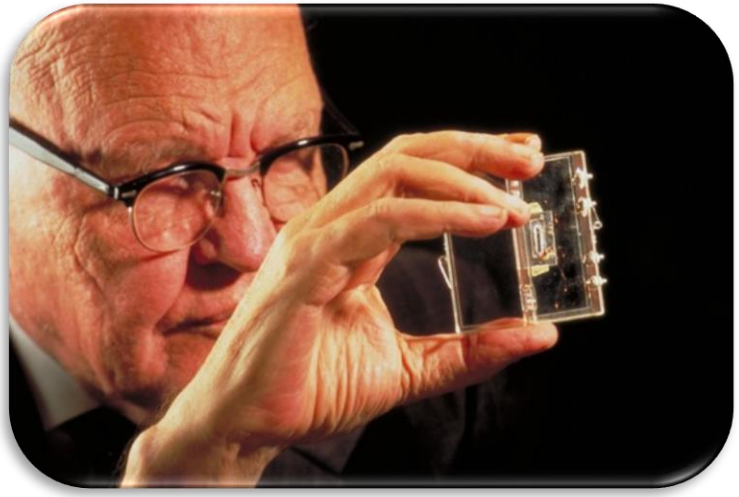
Approved for Public Release

Today's Talk

- Microelectronics Background and Threats
- Cyberspace Domain
- Hardware Assurance and Zero Trust
- Multi-layer Security
- Trusted Foundry and Trusted Suppliers
- Policy
- Systems Engineering Context
- Conclusion

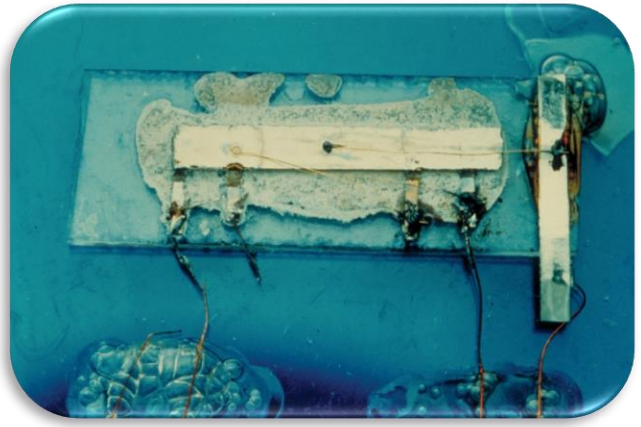
Approved for Public Release

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

Why Worry?

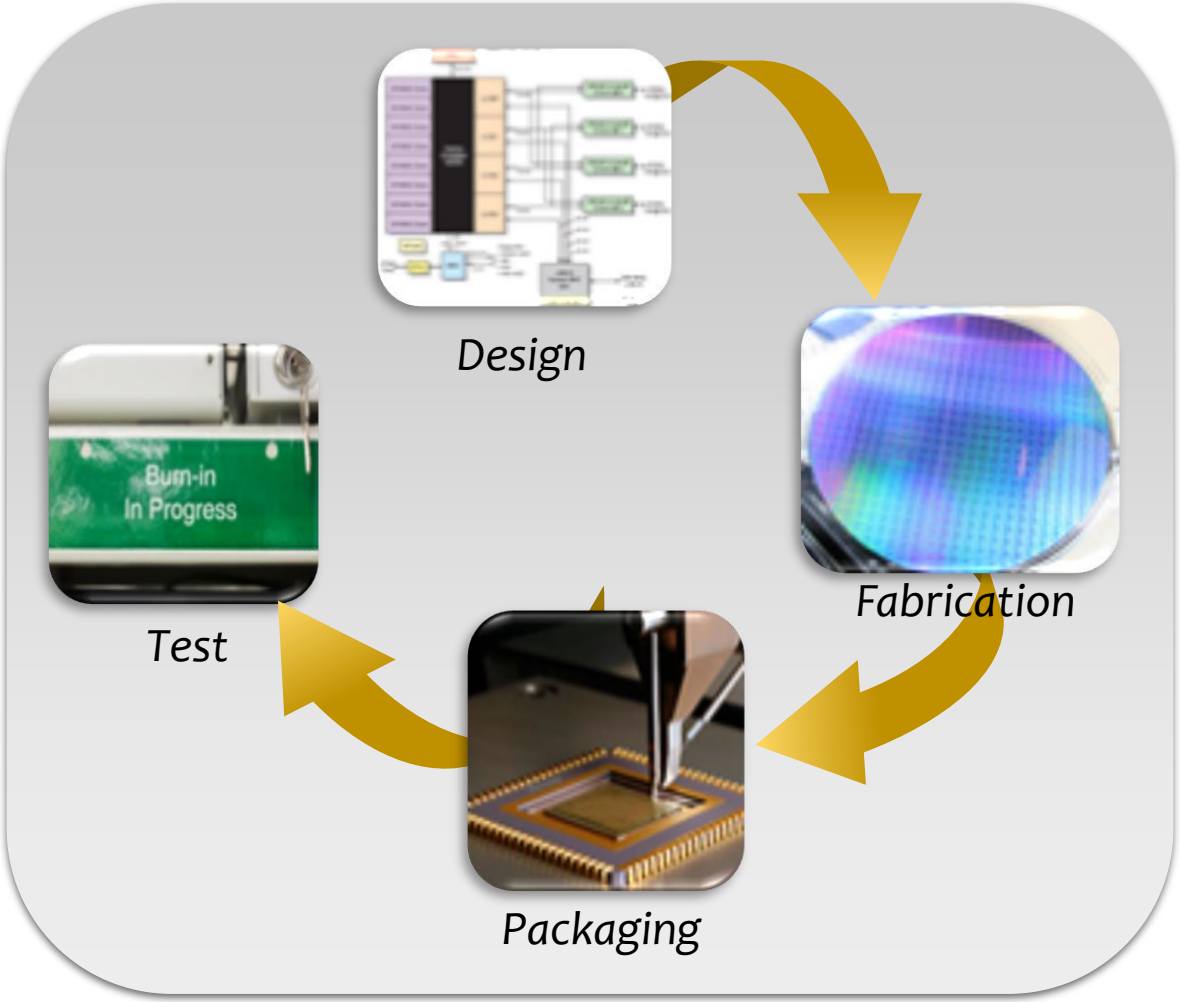
- *Over the past decades the United States has built an increasingly sophisticated suite of defense and intelligence capabilities . . .*

  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 multiple supply chain threats. . .*

  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.

Multiple Threats in Semiconductor Production Cycle



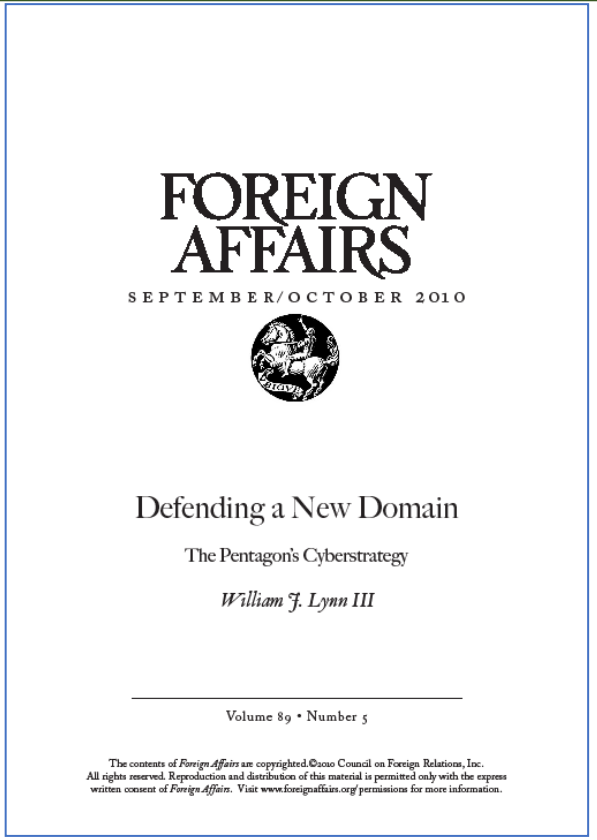
Risks:

- 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

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

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


FOREIGN AFFAIRS

SEPTEMBER/OCTOBER 2010

Defending a New Domain

The Pentagon's Cyberstrategy

William J. Lynn III

Volume 89 • Number 5

The contents of *Foreign Affairs* are copyrighted.©2010 Council on Foreign Relations, Inc. All rights reserved. Reproduction and distribution of this material is permitted only with the express written consent of *Foreign Affairs*. Visit www.foreignaffairs.org/permissions for more information.

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

Cyberspace Domain

Cyberspace is the digital infrastructure that enables our collective aspirations as a nation and includes people, technology (hardware and software), and doctrine

- Hon. Chris Inglis, National Cyber Director

- Microelectronics and software are the foundations of secure critical cyberspace infrastructure
  - All 16 critical national infrastructure sectors require hardware and software assurance for cyberspace resilience
  - When combined with physical security and proper authentication & authorization, using Trusted Suppliers enables multi-layered security

Approved for Public Release

Multi-layer Security – HwA + Cybersecurity

- 2008 Comprehensive National Cybersecurity Initiative (CNCI)
  - Initiative #11 - Develop a multi-pronged approach for global SCRM
  - Threat actor accesses system, alters its operation, and steals data
  - Exploits vulnerabilities remotely, inserted through supply chain
- In the last 20 years we have seen more -
  - Networked and software intensive systems, internet enabled-operational technology, IoT, off-shoring of chip production
- Cybersecurity includes protecting networks and data and physical systems (CISA ICT SCRM Task Force)
  - Cyber-physical systems blur the distinction and expand the attack surface
  - Zero Trust has become the catch phrase of today for ICT

Hardware assurance is more critical than ever, and more difficult

Zero Trust Principles - Always Verify

- Assume that threats (external and internal) are always present
- Explicitly and continuously verify every transaction
- Authentication and authorization across the enterprise
- ZTA principles for HwA can complement Trusted Supplier protections

Approved for Public Release

Multi-layer Security – HwA + Cybersecurity

- Zero Trust is necessary for IT infrastructure security (OSI Layer 7)
- Hardware supply chains are different (OSI Layer 1)
  - Design, manufacturing, packaging, test, procurement, distribution, integration, and sustainment (material sourcing to end use)
  - Complex, distributed, fragile and dynamic environment
- Assured hardware is critical the comprehensive system security required for mission success

Microelectronics from a Defense Microelectronics Activity (DMEA) accredited Trusted Supplier provide multi-layered security

Hardware Assurance (HwA)

- Confidence that microelectronics and embedded software function as intended and are free of vulnerabilities during the microelectronics life-cycle
- Program Protection Planning and Trusted and Secure Systems analysis
  - Requires early identification of Critical Program Information and components
  - Endorses Trusted Suppliers as viable mitigations
  - Leverages long-term C-I-A (confidentiality-integrity-availability) attributes of Trusted Suppliers

Multi-layer security combines trusted and assured hardware with cybersecurity measures

Approved for Public Release

DMEA Trusted Foundry and Trusted Supplier Program

Trusted - 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).

- DMEA Website /Trusted Program

- Within this context, "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 in supply
  - Prevent intentional or unintentional modification or tampering of the ICs
  - Protect the ICs from unauthorized attempts at reverse engineering, exposure of functionality or evaluation of their possible vulnerabilities

Approved for Public Release

Trusted Foundry and Trusted Supplier Program

- Provides important benefits for mission assurance
  - Selecting components from Trusted Suppliers mitigates the risk of technology corruption, tampering, cyber-attacks, and counterfeiting
  - Using Trusted Suppliers improves parts management for legacy systems by assuring access to supply well past the normal commercial product sunsetting practices
- Trusted Supplier will be an established mitigation in the Microelectronics Assurance Framework
  - DMEA accreditation is being mapped to custom microelectronics threat space and existing guidance

When used in conjunction with ZTA principles, Trusted Microelectronics can provide comprehensive, multi-layer risk-based security

Defense Microelectronics Activity (DMEA)

- Program Manager for the DoD Trusted Foundry program
  - Provides a cost-effective means to assure the confidentiality, integrity and availability of integrated circuits during design and manufacturing
  - Provides US Government offices with access to leading edge, state-of-the-practice, and legacy microelectronics for national security applications
- DMEA has been designated as the DoD Center for Industrial Technical Excellence (CITE) for defense microelectronics
  - Allows greater utilization of DMEA resources
  - Leverages public-private cooperative arrangements
  - Enables partnering among depots/arsenals and private industry
  - Enhances DoD's ability to provide support to critical warfighting capabilities

Approved for Public Release

Defense Microelectronics Activity

Pillars of DMEA

Trusted Access Program Office (TAPO)	Ensure access to cutting-edge microelectronics and accredit Trusted Suppliers
Advanced Technical Support Program (ATSP)	Accelerate microelectronics acquisition and provide technical oversight
Organic Engineering	Provide flexible, full-spectrum microelectronics solutions
Radiation Testing	Deliver secure, cost-effective radiation qualification testing and research

Approved for Public Release

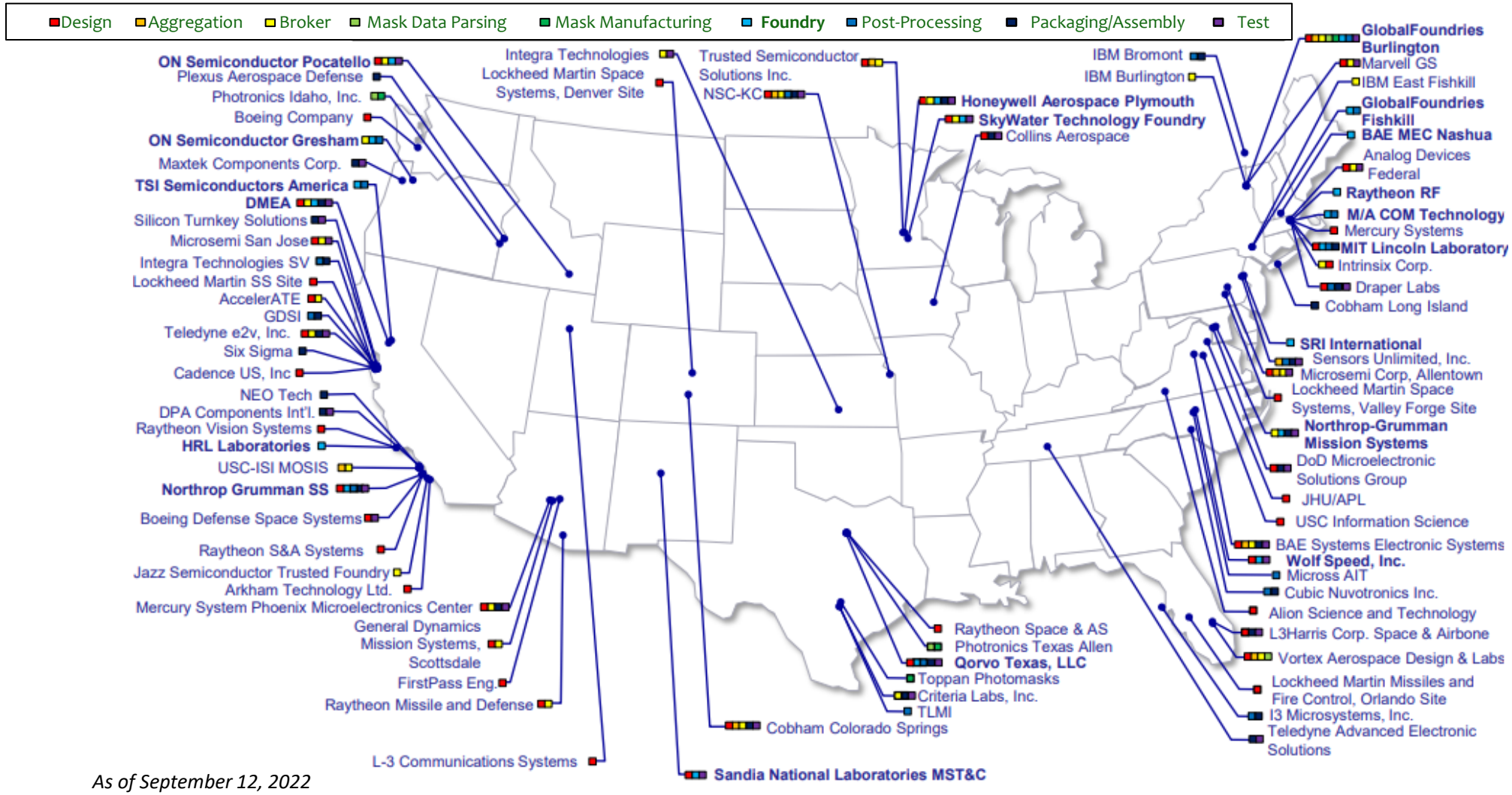
Trusted Access Program Office

- TAPO facilitates and administers the contracts and agreements with industry to provide US Government users with
  - Advanced foundry services including multi-project wafer (MPW) runs, dedicated prototypes, and production in both high- and low-volume models
  - A library of standard IP blocks (most margined down to the Mil-Std-Temp range)
  - Packaging and test services
  - Accredits suppliers per DoDI 5200.44

Trusted Foundry program provides the US Government with guaranteed access to advanced, state-of-the-practice, and legacy Trusted microelectronics for the typically low volume needs of government programs.

Approved for Public Release

80 Trusted Suppliers



As of September 12, 2022

Approved for Public Release

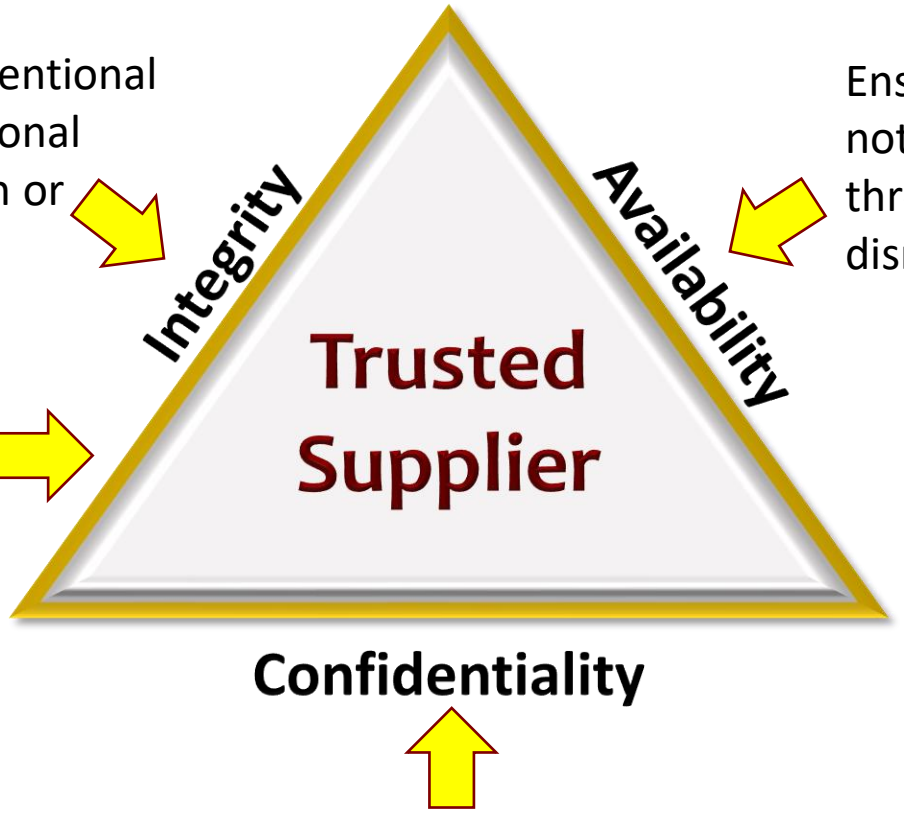
Trusted Suppliers Products and Services Offered

- 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
- Trusted microcircuit emulation
- Anti-cloning protection
- Trusted photomask development and parsing
- Trusted ASIC and FPGA design and broker services

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

Approved for Public Release

Benefits of Using Trusted Suppliers



Prevents intentional or unintentional modification or tampering

Ensures that there will not be any reasonable threats related to disruption of supply

Provides an assured "Chain of Custody" for both classified and unclassified components

Protects components from unauthorized attempts at reverse engineering, exposure of functionality or evaluation of their possible vulnerabilities

Approved for Public Release

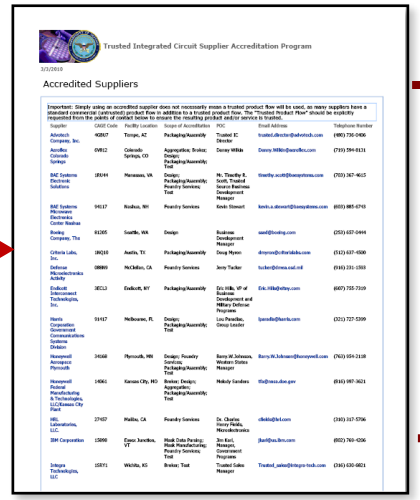
Trusted Microelectronics Options

Trusted IC Requirement

State-of-the-Practice or Legacy?

Determine Trusted products and services needed

Review Trusted Accredited Suppliers (TAS) capabilities


Trusted Integrated Circuit Supplier Accreditation Program

Accredited Suppliers

Supplier services and POCs listed on DMEA website

Initiate direct engagement with one or more TAS

- OR -

Initiate direct engagement with aggregator or broker

State-of-the-art Leading Edge?

TAPO
Trusted Access Program Office

Government Sponsor

Explicitly request Trusted Flow at each stage of engagement

Goal of Technology and Program Protection Policy

- Protect mission critical components (hardware, software, firmware)
  - Software assurance (SwA)
  - Hardware assurance (HwA)
    - Trusted/assured microelectronics
- Consideration of Trusted Suppliers begins early in development
  - Identify notional critical functions to implement with microelectronics
  - Trade studies should include C-I-A attributes of Trusted Suppliers
  - TSN analysis to identify ASICs and applicability of DODI 5000.44
- Program offices can incorporate requirement in RFPs and SOWs
  - Include the requirement for a Trusted Process Flow in the solicitation, directing the use of a DMEA-accredited Trusted Supplier

Approved for Public Release

Mission Critical Microelectronics Policy

- DoDI 5200.44 - Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)

> ***"In applicable systems, integrated circuit-related products and services shall be procured from a trusted supplier accredited by the Defense Microelectronics Activity (DMEA) when they are custom-designed, custom-manufactured, or tailored for a specific DoD military end use (generally referred to as application-specific integrated circuits (ASICs))."***

- Applicability
  - All mission critical functions and critical components within applicable systems identified through a criticality analysis, including spare or replacement parts

Approved for Public Release

Mission Critical Microelectronics Policy

- Other applicable instructions
  - DoDI 5000.83 - Technology And Program Protection To Maintain Technological Advantage
  - Technology and Program Protection (T&PP) Guidebook (July 2022) https://rt.cto.mil/wp-content/uploads/TPP_Guidebook_Jul2022_cleared.pdf
  - DoDI 5200.39 - Critical Program Information (CPI) Identification and Protection Within Research, Development, Test, and Evaluation (RDT&E)
  - DoDI 5200.47 - Anti-Tamper (AT)
  - DoDI 4140.67 - DoD Counterfeit Prevention Policy
- Inclusion in contracts
  - For policy to have effect program offices should include applicable provisions in contractual documents and requirements

Approved for Public Release

Systems Engineering Decision Points

- Trade studies should include early assessment of use of Trusted Suppliers for microelectronics
  - When defining alternative system concepts or configuration items determine if microelectronics from a Trusted Supplier can be used to provide desired functionality
- Program Protection Plan identifies Critical Program Information
  - Trusted Suppliers' Trusted Flow is adequate to protect Critical Program Information as required by DODI 5200.39, Critical Program Information (CPI) Protection Within the Department of Defense
  - An ASIC with a CPI designation should be sourced from a Trusted Supplier

Approved for Public Release

Conclusion

- Programs should understand when to select components from Trusted Suppliers during their system development
- Engineers should factor benefits into program protection systems security engineering planning and protocols
- Programs should engage with TAPO and Trusted Suppliers early to ensure products and services are accessed
- The Trusted Foundry and Trusted Supplier Programs are key resources for defense programs

Approved for Public Release

Contacts

DMEA – DOD Program Management & Accreditation

tapo@dmea.osd.mil

DBS – Outreach (contractor)

dchesebrough@definedbusiness.com

Approved for Public Release