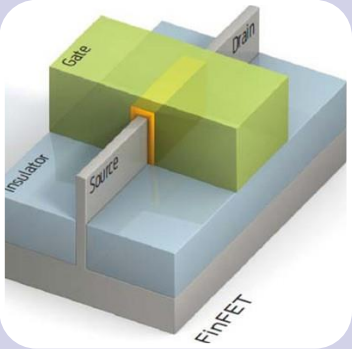
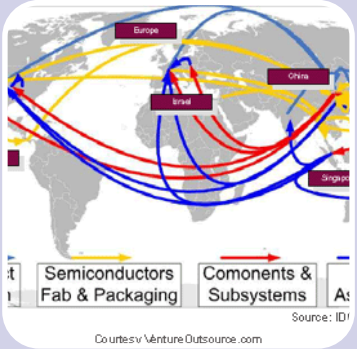
Long-Term Strategy for DoD Trusted and Assured Microelectronics Needs

Jeremy Muldavin, Ph.D.
Office of the Deputy Assistant Secretary of Defense for Systems Engineering

20th Annual NDIA Systems Engineering Conference
Springfield, VA | October 26, 2017

Microelectronics Trends





State-of-the-art Devices

- Deeply-Scaled Silicon ICs (10nm)
- 2.5 & 3D ICs
- Heterogeneous System-on-Chip (SoC) ICs
- Flexible and miniature packaging
- Accelerator and SoC architectures

Increasing Cost and Complexity

- $5-15B for a modern fabrication facility
- >$500M for a new commercial smart phone SoC development
- Reliance on third-party Intellectual Property (IP)
- No one can do it alone

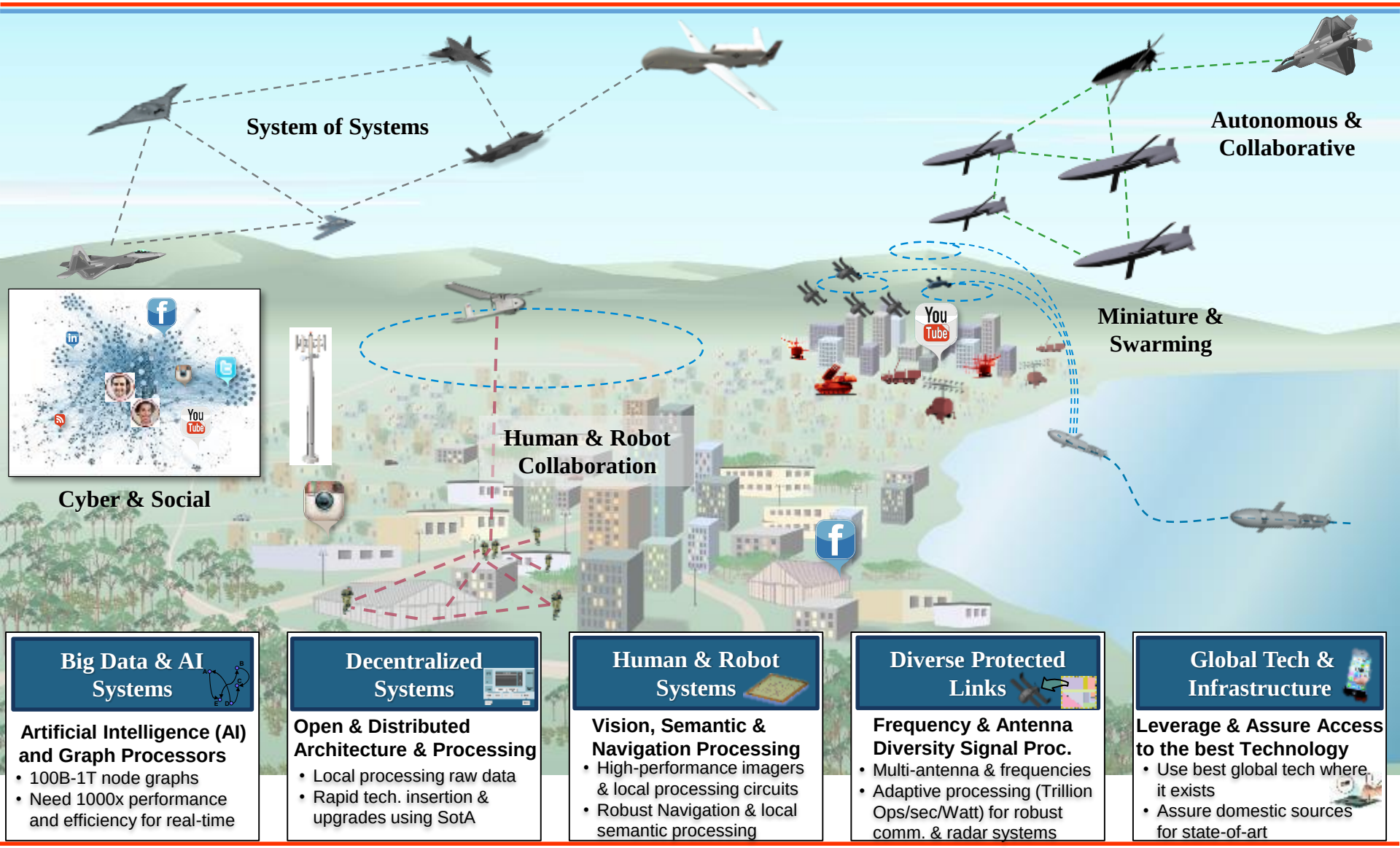
Globalization and Commercial Dominance

- State-of-the-art fabrication consolidation
- Commercially driven (DoD <1% of market)
- Complex global supply chain
- China ($150B) & Saudi Arabia ($100B) investing heavily

New Applications

- Internet of Things
- Big Data systems
- Autonomous systems
- Spectral and spatial communication agility
- Government & Defense need all of above with higher security & performance

Future Warfighting Systems
Advanced Microelectronics Needs



Big Data & AI Systems

Artificial Intelligence (AI) and Graph Processors

- 100B-1T node graphs
- Need 1000x performance and efficiency for real-time

Decentralized Systems

Open & Distributed Architecture & Processing

- Local processing raw data
- Rapid tech. insertion & upgrades using SotA

Human & Robot Systems

Vision, Semantic & Navigation Processing

- High-performance imagers & local processing circuits
- Robust Navigation & local semantic processing

Diverse Protected Links

Frequency & Antenna Diversity Signal Proc.

- Multi-antenna & frequencies
- Adaptive processing (Trillion Ops/sec/Watt) for robust comm. & radar systems

Global Tech & Infrastructure

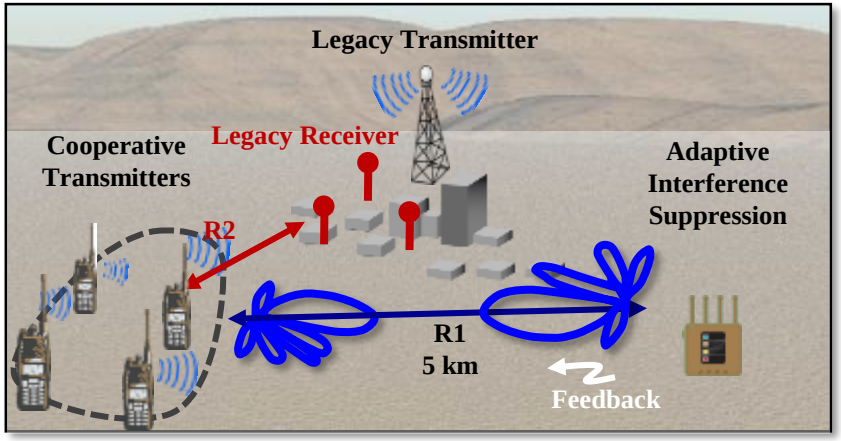
Leverage & Assure Access to the best Technology

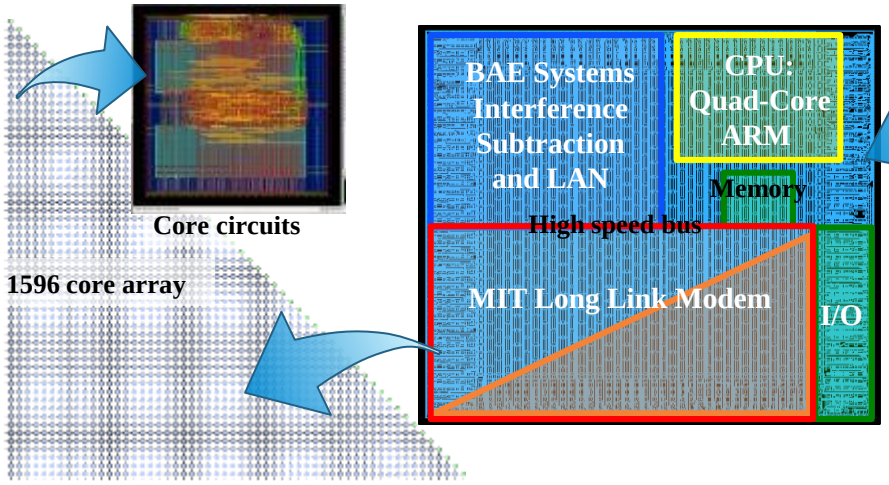
- Use best global tech where it exists
- Assure domestic sources for state-of-art

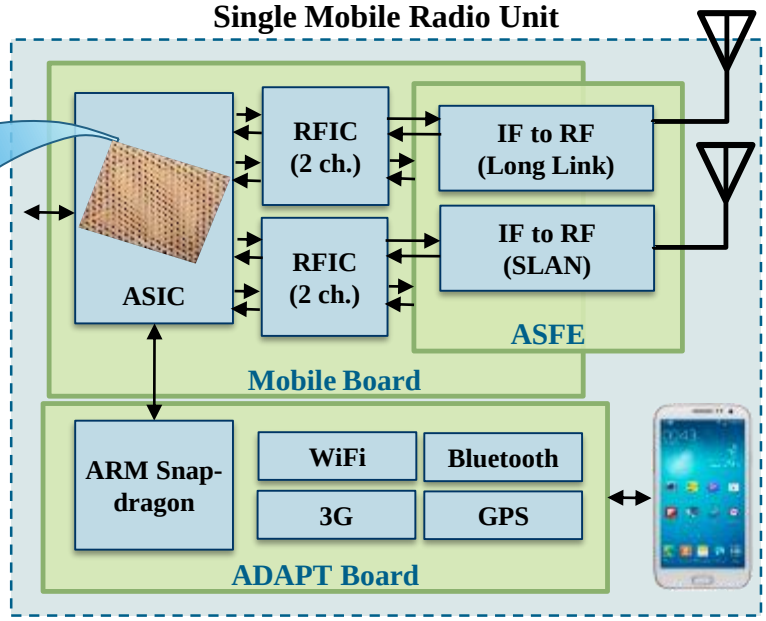
A DoD System on Chip Example

Leverages extreme ASIC computational technologies

- Coherent beam forming, adaptive nulling and interference cancellation:
  - 5-10x range extension or 1000x lower power
  - 10000 interferer to signal ratios
- Mobile radio form factor achieved by ASIC accelerators with 1.7 TOPS/W



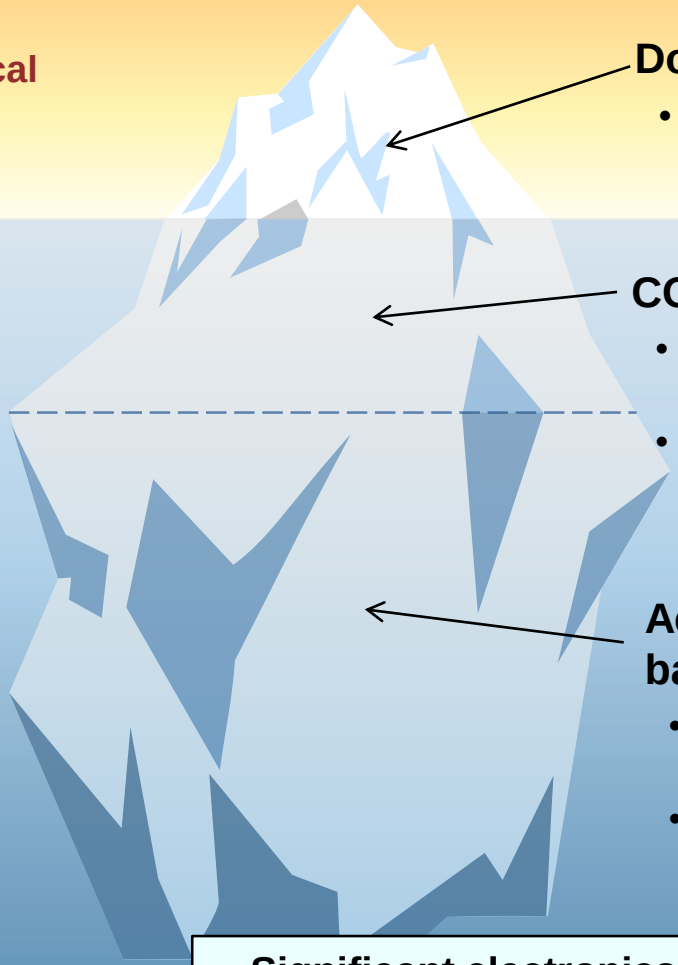




1.7 TOPS/W System on Chip for MIMO Communications Applications

Electronics as a Strategic Issue

Current Tactical Issue



Larger Strategic Issue

DoD Trusted Electronics Issue

- **Options for domestic trusted manufacture of custom DoD electronics are diminishing**

FY03-16 Trusted Foundry Program

COTS Electronics Trust (DoD & Beyond†)

- **Most COTS electronics used in DoD systems are fabricated overseas; significant risk from tamper**
- **Risks similar for the broader national security community, banking, critical infrastructure, etc.**

PB 17: Trusted & Assured Micro-electronics

Access to Electronics / Electronics based economic growth

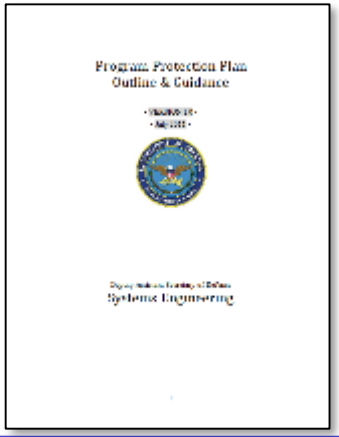
- **Shift in electronics fabrication creates potential for overseas control**
- **End of Moore's Law potential carries economic impacts**

POM 19-23: Micro-electronics Innovation for National Security

Significant electronics challenges represent a strategic level national issue

† Including the broader national security community, banking, critical infrastructure, commercial industry, etc.

What We Are Doing

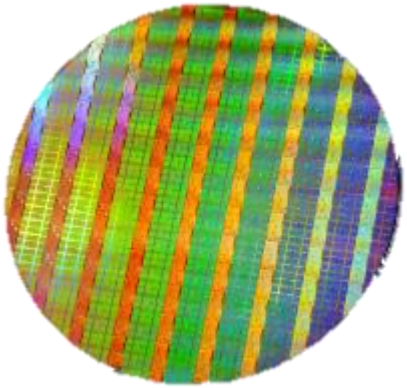


Policy

- DoD Instruction (DoDI) 5000.02
- Program Protection Plan (PPP)
- International Traffic in Arms Regulations (ITAR) update (in work)

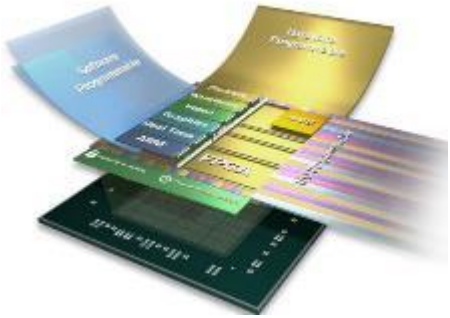
Joint Federated Assurance Center

- Software assurance knowledge & tools
- Hardware assurance knowledge & tools
- Advanced verification & validation capabilities



Trusted & Assured Microelectronics

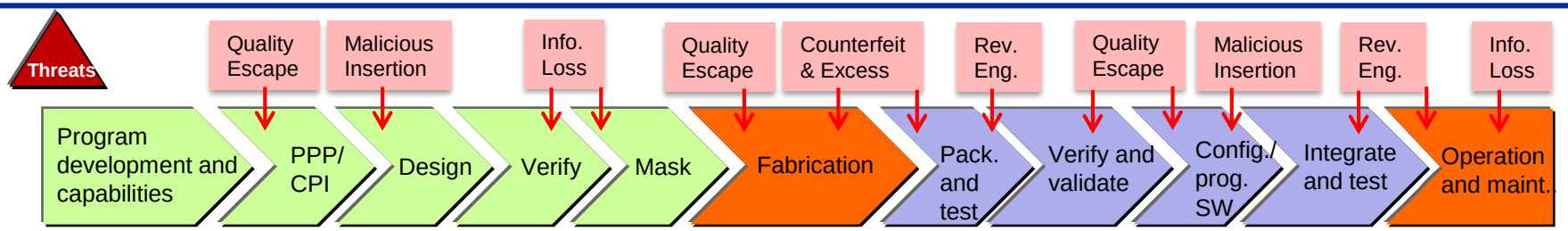
- Access to state-of-the-art foundries
- Trust and assurance methods and demonstration
- Industrial best practices for assurance



COTS and FPGA

- Supply chain risk management
- FPGA Assurance Study
- Radiation-hardened microelectronics initiative

Systems Engineering Approach



JFAC & Industry

Efficacy

Impact

Mitigation

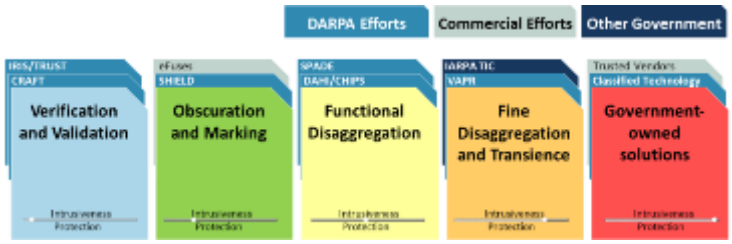
Innovators & Developers

System architects

R&D engineers

Acquisition experts

Manufacturing experts



Adopters & Improvers

System integrators

Test and validation

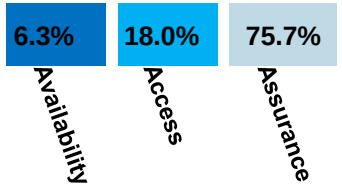
Operators and maintainers

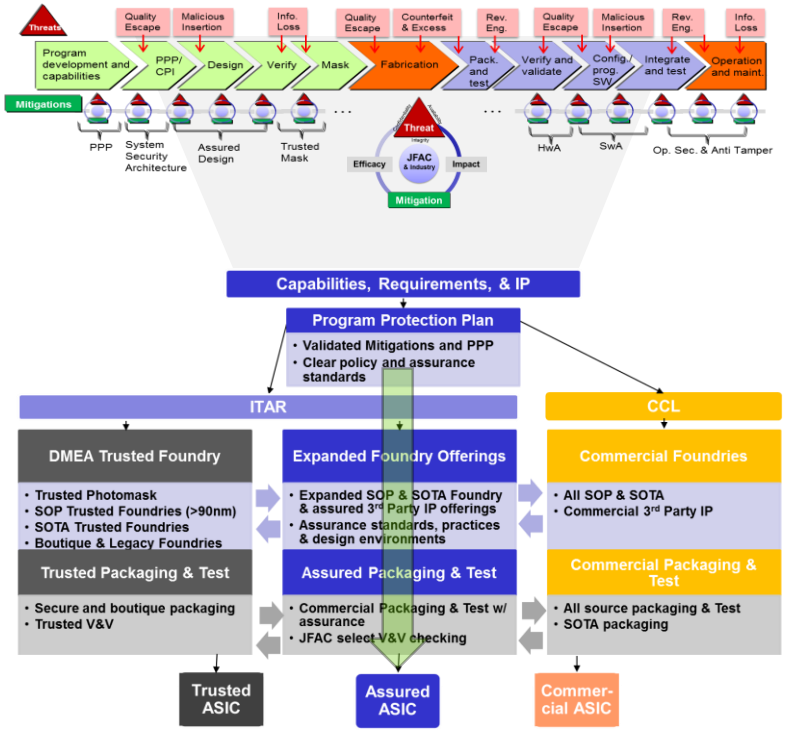
Trusted & Assured Microelectronics FY18 Activities and Investments

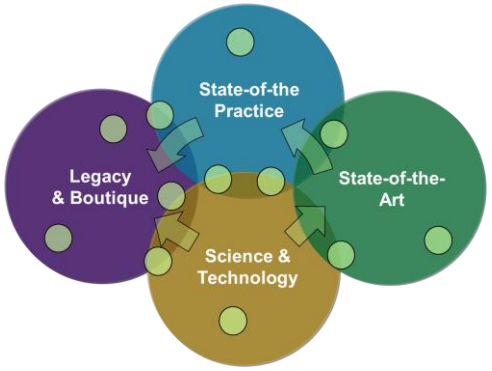
Overall

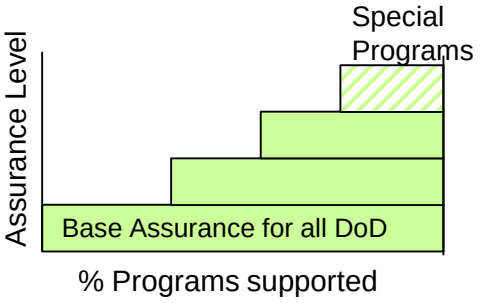
Inputs	Investments & Actions	Deliverables & Outcomes
• DARPA, IARPA, & Commercial Assurance Technologies • JFAC Labs, DMEA, FFRDCs • DoD Programs & Commercial Suppliers	• Develop, Mature and demonstrate Assurance Mitigations • Evaluate Effectiveness of protections of IP and Integrity • Support trusted mask fabrication • Transition to & support programs	• List of Validated mitigations and V&V capabilities • PPP and mitigation guides and best practices • Program demonstration support and trusted mask creation • Special program V&V support

FY18 Funding Distribution



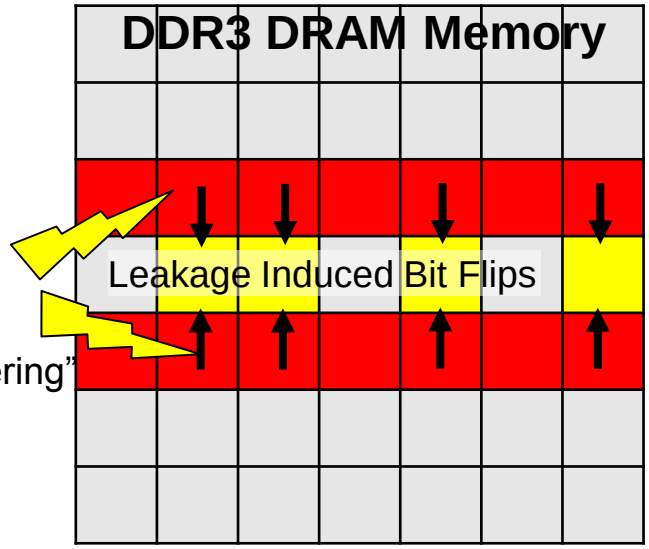






Examples of Recent Cyber Attacks on HW Vulnerabilities

- **Rowhammer Attack**
  - Fault in DDR3 DRAM modules
  - High integration density allows leakage current to neighbor rows on readout
  - Rowhammer induces frequent readout to intentionally force bit flips in adjacent transistor rows.
  - **Effects**: Loss of Data, Loss of Reliability, Privilege Escalation



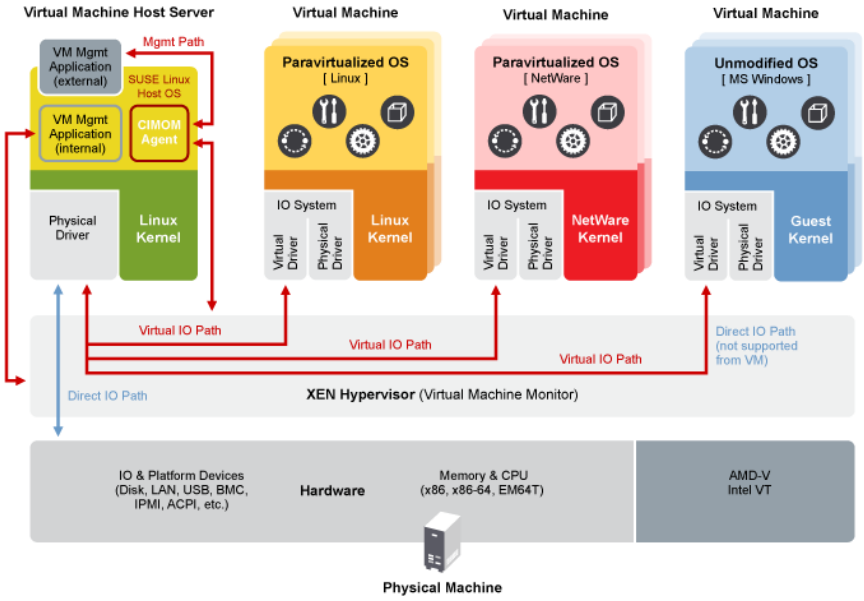
- **Cyber attack on Smart Phones with Adups Firmware (FW)**
  - FW uses HW to perform data exfiltration of texts and personal data, enabling Chinese gov't to monitor citizens
  - Very weak security protections enabled exploitable FW to be loaded on American Smart Phones.
  - **Effects:** Millions of smartphones affected worldwide and devices geographically targeted thru GPS data

Reference:<https://en.wikipedia.org/wiki/Row_hammer>
Reference:<https://www.nytimes.com/2016/11/16/us/politics/china-phones-software-security.html?_r=2>

Mitigations to Cyber Exploits of HW Vulnerabilities

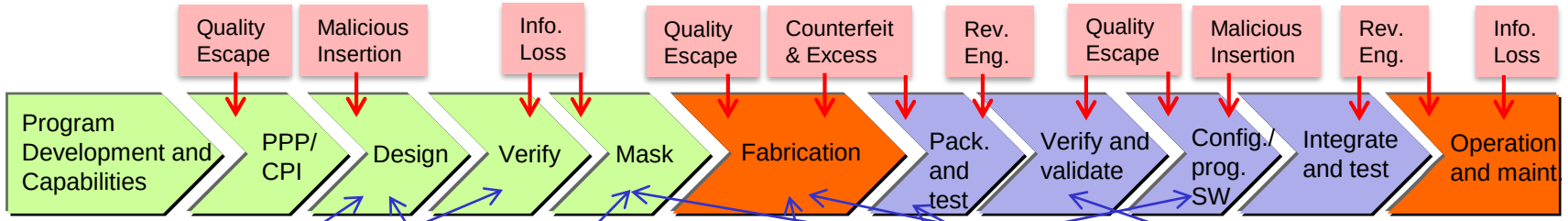
- **Root of trust (ROT)**
  - Encryption of data
  - Monitoring for unauthorized operations
  - Detection of attempts to root a device
  - Memory security partition management
  - Digital rights management
- **Embedded Hypervisor Enforces Security Rules from ROT**
  - Requires only signed SW and FW can be loaded onto HW
  - Controls authentication and setup of initial system state to restrict unauthorized access to HW
- **Monitoring Software**
  - Software that observes execution of the system
  - Alerts to any unauthorized behavior

XEN Hypervisor Implementation



Reference:<http://www.novell.com/documentation/vmserver/virtualization_basics/data/ba0khrq.html>

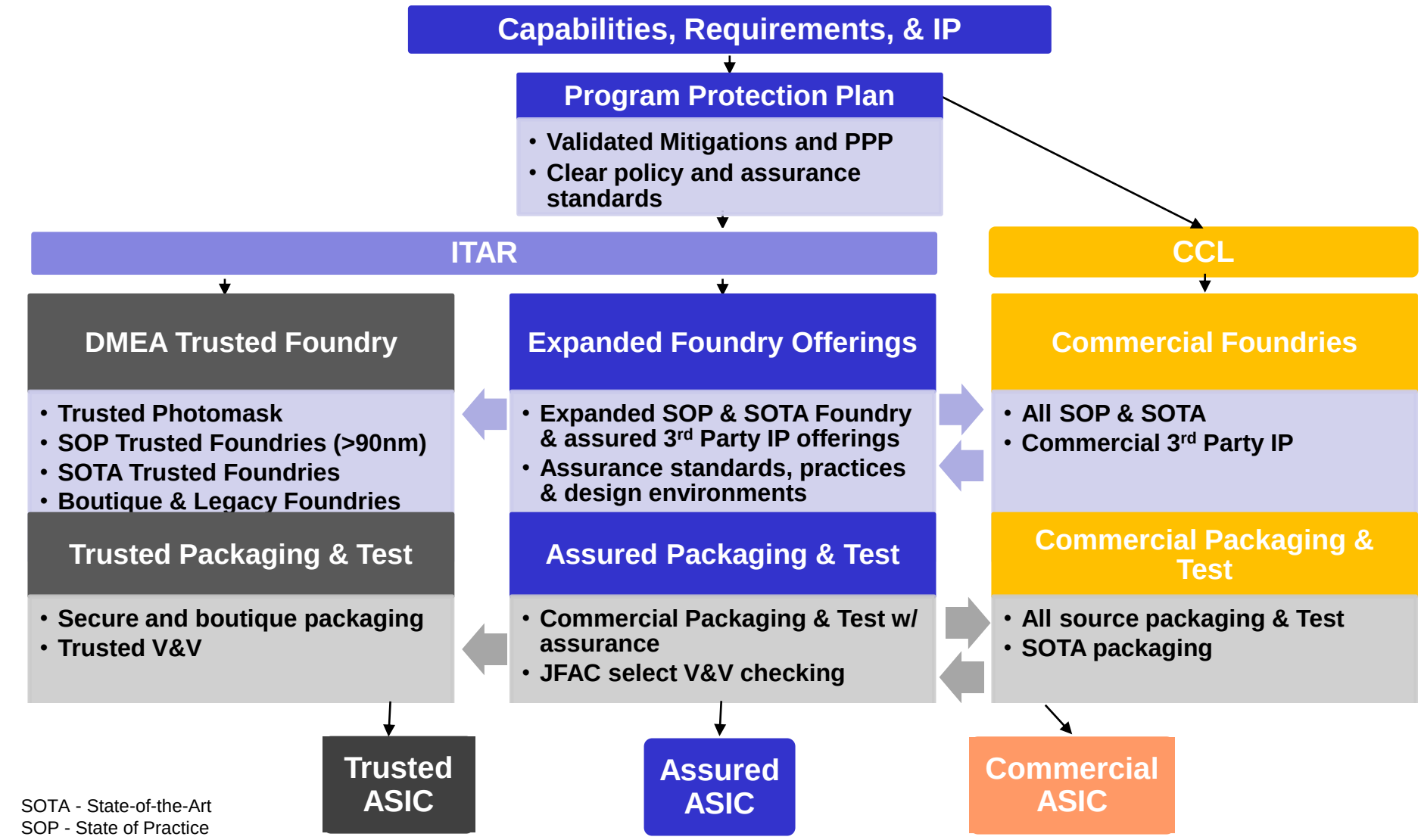
New Trust and Assurance Approaches



Design for trust	IP protection	Low-volume/high-mix production	Electronic component markers	Imaging technologies and forensics
• Designing techniques to limit full use/functionality to trusted operation	• Preventing exploitation, including control of use, concealment, reconfiguring, partitioning, or employment	• Innovative methods to permit cost-effective, Trusted and assured low volume manufacturing of state-of-the-art ICs	• Tagging/marking ICs and subassemblies to authenticate and track supply chain movements	• Advanced capabilities to efficiently evaluate dense, state-of-the-art commercial components

Implement and demonstrate assurance capability with transition partners

Potential Paths to ASIC Production for DoD



SOTA - State-of-the-Art
SOP - State of Practice

T&AM Focus Areas

Verification & Validation

- Improves microelectronics test and verification methodologies in support of verifying the trust and assurance of parts

Design Assurance

- Assured and immediate access to domestic production of advanced microelectronics and disruptive research and development investments to surpass the impending limitations of Moore's Law on silicon microelectronics

FPGA Assurance

- Demonstrate innovative design, manufacturing, imaging, tagging, control and assessment approaches for protecting DoD's microelectronics supply chain and intellectual property

Enhanced Manufacturing

- Development of advanced node microelectronics fabrication and packaging capabilities at existing SOTP foundries with a focus on high-mix, low-volume alternatives

Radiation Hardened Microelectronics

- Demonstrate innovative design, manufacturing, and assessment approaches for trusted, strategic radiation-hardened electronics in advanced technology nodes for next-generation strategic systems

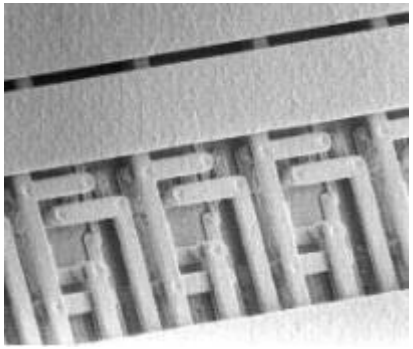
Outreach & Standards

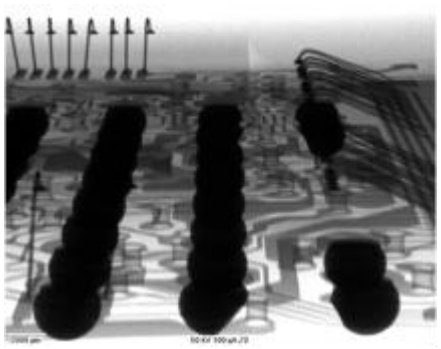
- Develop standards and practices to foster commercial development of secure, trusted and assured parts.
- Document and promulgate security-enhancing design practices across government, industry, and academia

Microelectronics Trust Verification Technologies

- **Verification needed when Trusted Foundry not available**
  - DoD formed JFAC to provide this service
  - Long-term challenge to analyze leading-edge ICs and scale up capacity

Design Verification	Physical Verification	Functional Verification
• Verification/assurance of designs, IP, netlists, bit-streams, firmware, etc.	• Destructive analysis of ICs and Printed Circuit Boards	• Non-destructive screening and verification of select ICs





DoD, Intelligence Community, and DoE enhancing capability to meet future demand

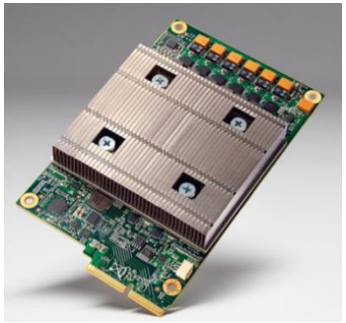
Verification & Validation: Survey Status and Initial Results

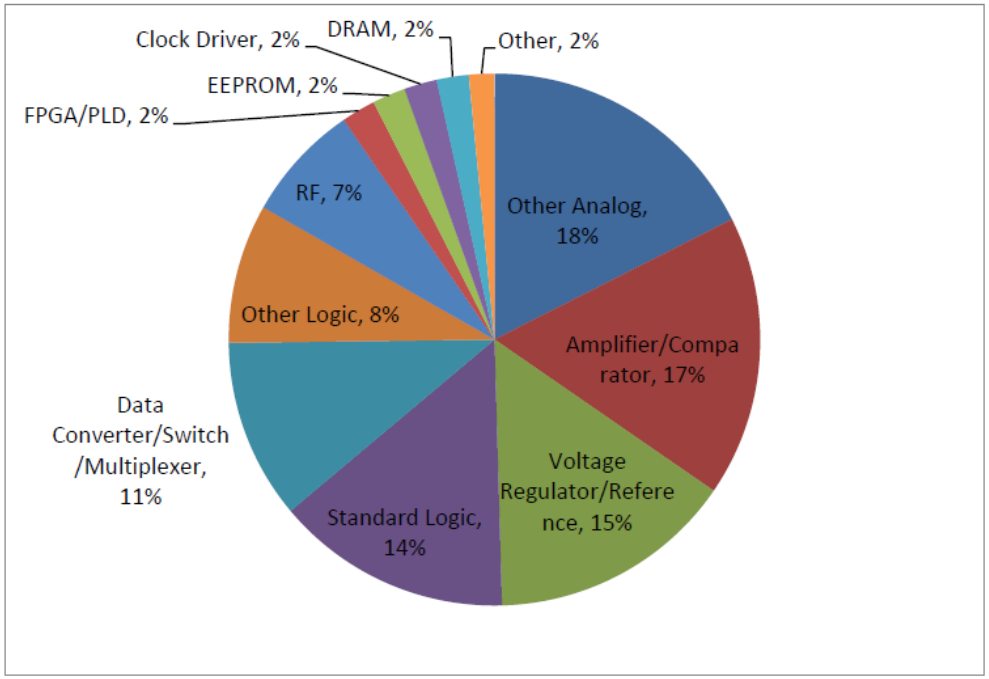
Data obtained from:

- Programs (early production and pre-production) based on BOMs
- Commercial Assemblies bases on BOMs
- Programs that have completed prioritized usage survey
- Companies that have completed prioritized usage survey
- S&T Programs that have completed prioritized usage survey

NVIDIA Tesla GPUs
15.3 Billion transistors IC

Google's Tensor Processing Unit could advance Moore's Law 7 years into the future



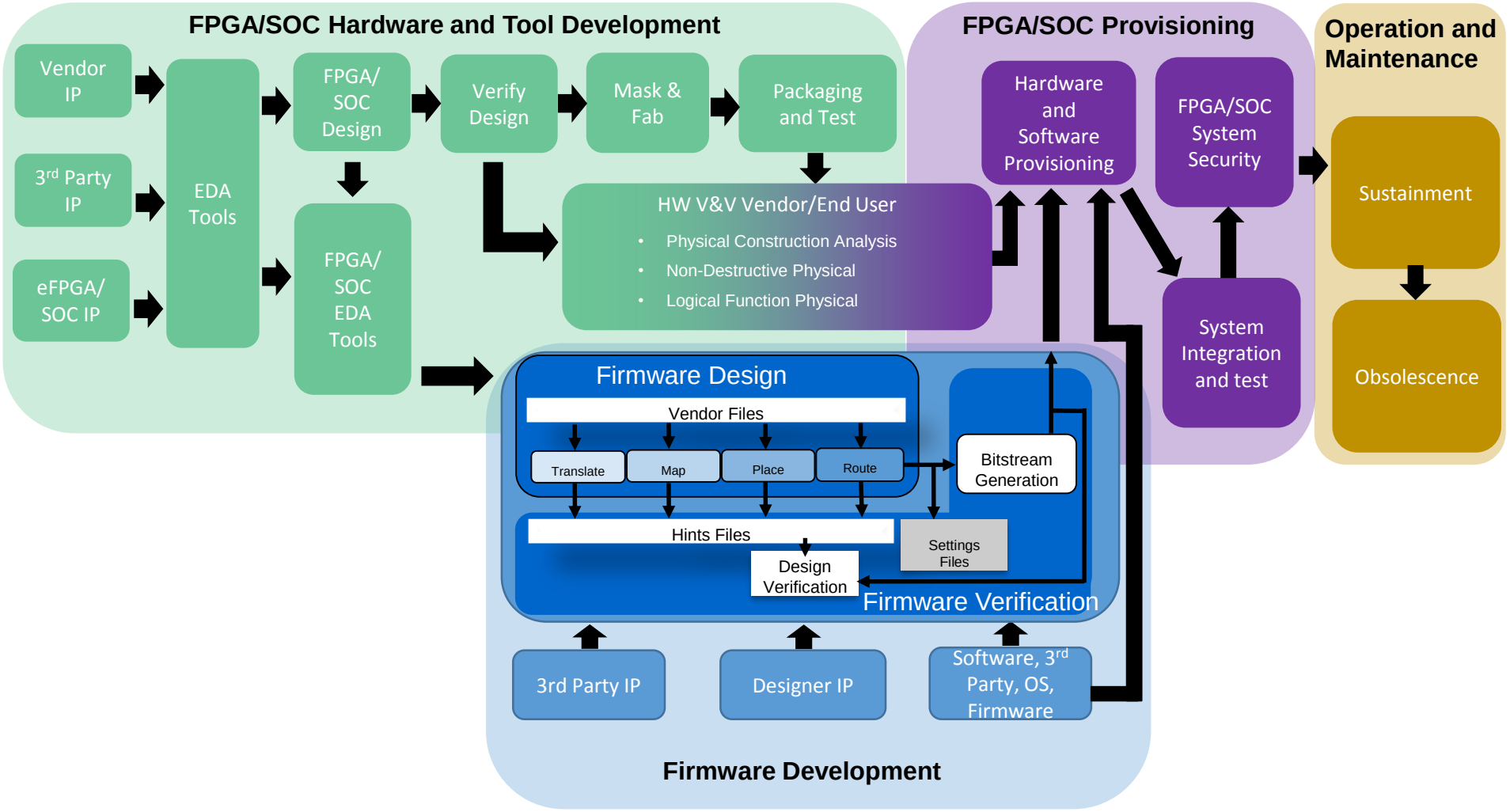


Above chart curtesy IDA report, *Examination of DoD's Use of Microelectronics in Weapon Systems*, 2013

Outreach and Industry Standards

- **JFAC Standards and Best Practices Sub Group**
  - Establish a charter to be reviewed and approved by JFAC, T&AM and Service/Agency communities
- **Evaluate COTS methods and realistic/practical alternatives for attaining trustworthiness**
  - Extension and application of the Trustworthy Supplier Framework
- **Develop and expand the NDIA Collaboration**
  - Work towards the establishment of the “Electronics Division”
    - Shared government liaison – DASD(SE), DMEA, DASD(MIBP) and NRL on behalf of the MEC MWG
  - Continue building community, workshops and meetings – build the NDIA Electronics as a central focus for industrial dialog with the government
- **Collaboration and Information Sharing**
  - Pilot with FPGA Assurance and the JFAC Standards Group - Collaboration models, Information sharing
  - IntelDocs on Intelink for FOUO/Unclass (NIPR)
  - Pilot Standards Information Sharing on IntelDocs
  - IDA Sharepoint for Unclass/US citizen (TM JWG and Trust Models)
- **Outreach – Education, Training and Awareness**
  - Develop a long-term plan and near term FY18 goals
  - Build outreach materials for awareness of the FJAC and HwA
  - Coordinate T&AM efforts for outreach
- **Coordination**
  - Coordinate government wide HwA and T&AM activities
  - A single POC for common announcements, questions and interfaces with government, industry and academia
  - Active coordination and collaboration of T&AM related Conferences and Meetings
    - GOMACTech, HOST, MIM, FICS, etc.

FPGA/SOC Lifecycle Map

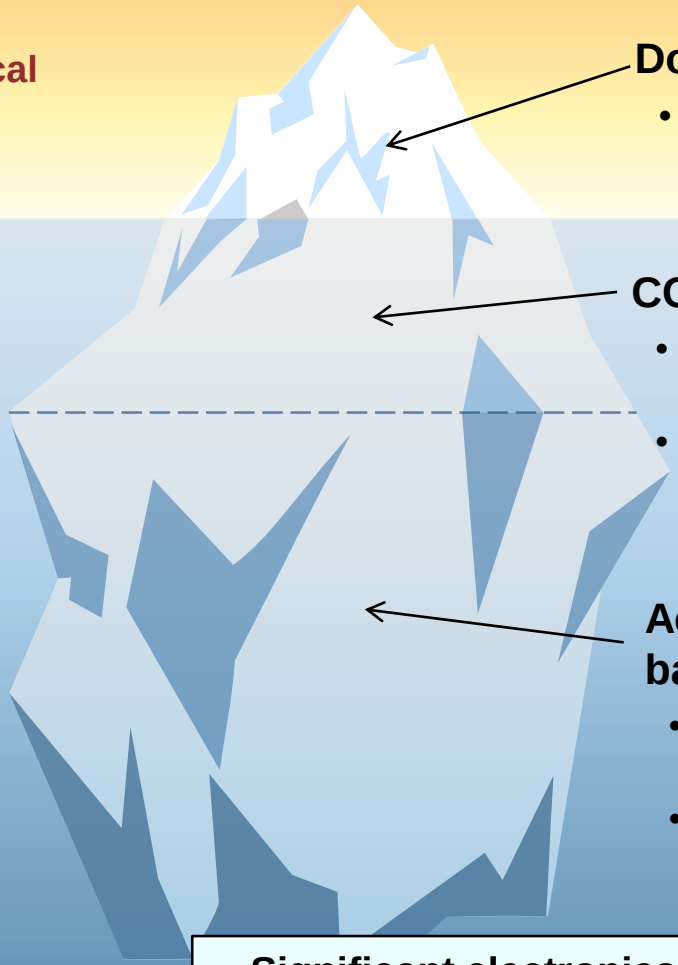


Pursuing Multiple Focus Areas Across the FPGA Lifecycle

	FPGA/SoC Hardware Development	FPGA/ Firmware Development	FPGA/SoC Provisioning	Operation & Maintenance
Policy	Adopt policy to promote best practices across acquisition programs			
Independent Verification And Validation	Expand IV&V capability and capacity for Physical, Functional and Design Verification To be offered to the			
New Technology	Development of new techniques to verify and validate protect IP Confidentiality, deliver advanced supply chain tracking technology and			
Supply Chain Threat	Enhanced interaction with the Intelligence Community to provide more specific threat information to better enable risk analysis and Risk Analysis			
Industry Engagement	Manufacturers' relations are critical: • IV&V requires timely and detailed design related information, • Design tool distribution and usage • Design verification features in the design or enabled by the design tools			
Leverage Related Efforts	Coordinate with Major Efforts across DOD and IC Communities: • Title III Trusted FPGA • Trust in FPGA Study • Aerospace TOR Guidance			

Electronics as a Strategic Issue

Current Tactical Issue



DoD Trusted Electronics Issue

- **Options for domestic trusted manufacture of custom DoD electronics are diminishing**

FY03-16 Trusted Foundry Program

COTS Electronics Trust (DoD & Beyond†)

- **Most COTS electronics used in DoD systems are fabricated overseas; significant risk from tamper**
- **Risks similar for the broader national security community, banking, critical infrastructure, etc.**

PB 17: Trusted & Assured Micro-electronics

Larger Strategic Issue

Access to Electronics / Electronics based economic growth

- **Shift in electronics fabrication creates potential for overseas control**
- **End of Moore's Law potential carries economic impacts**

POM 19-23: Micro-electronics Innovation for National Security

Significant electronics challenges represent a strategic level national issue

† Including the broader national security community, banking, critical infrastructure, commercial industry, etc.

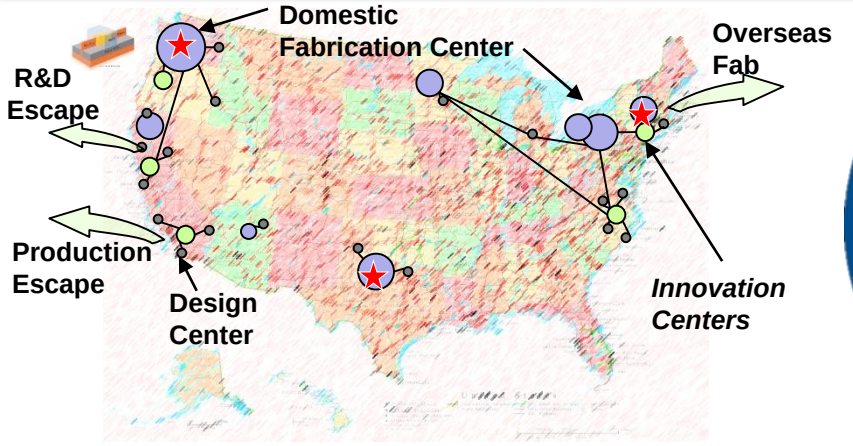
NDAA Strategy Request

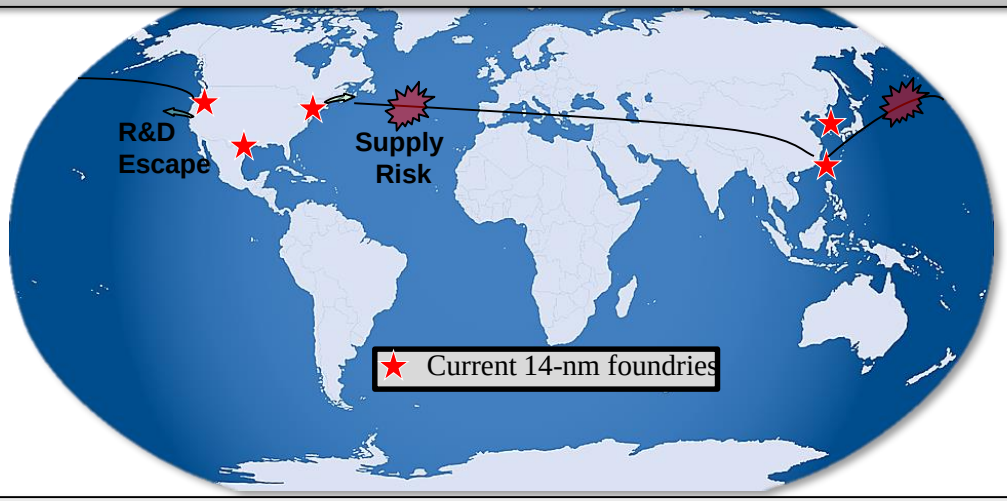
1. Define the various levels of trust required by DoD systems
2. Identify means of classifying DoD systems based on the required level of trust for microelectronics within the system
3. Identify means by which trust in microelectronics can be assured
4. Identify a means to increase the supplier base for assured microelectronics to ensure multiple supply pathways
5. Provide an assessment of the microelectronics needs of the DoD in future years, including the need for trusted, radiation-hardened microelectronics
6. Provide an assessment of the microelectronics needs of the DoD that may not be fulfilled by entities outside the DoD
7. Identify the resources required to assure access to trusted microelectronics, including infrastructure workforce, and investments in science and technology
8. Develop a research and development strategy to ensure that the DoD can, to the maximum extent practicable, use state of the art commercial microelectronics capabilities or their equivalent, while satisfying the needs for trust
9. Develop recommendations for changes in authorities, regulations, and practices, including acquisition policies, financial management, public-private partnership policies, or in any other relevant areas, that would support the achievement of goals of the strategy

Source: National Defense Authorization Act for Fiscal Year 2017, Section 231

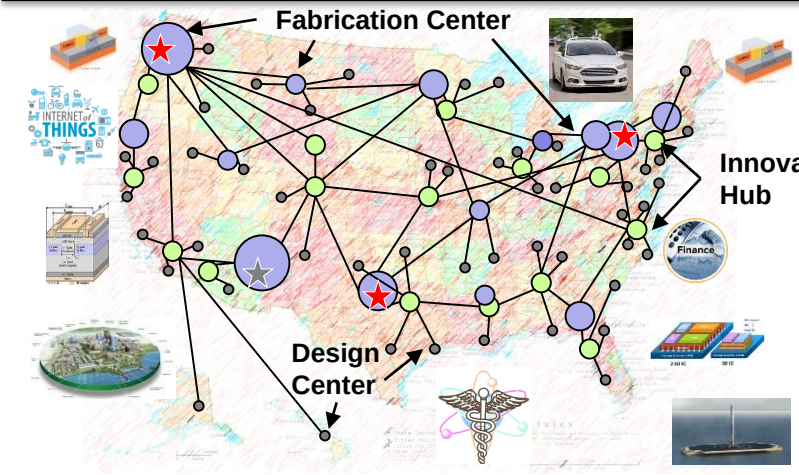
Leverage and Dominate Microelectronics for US Interests

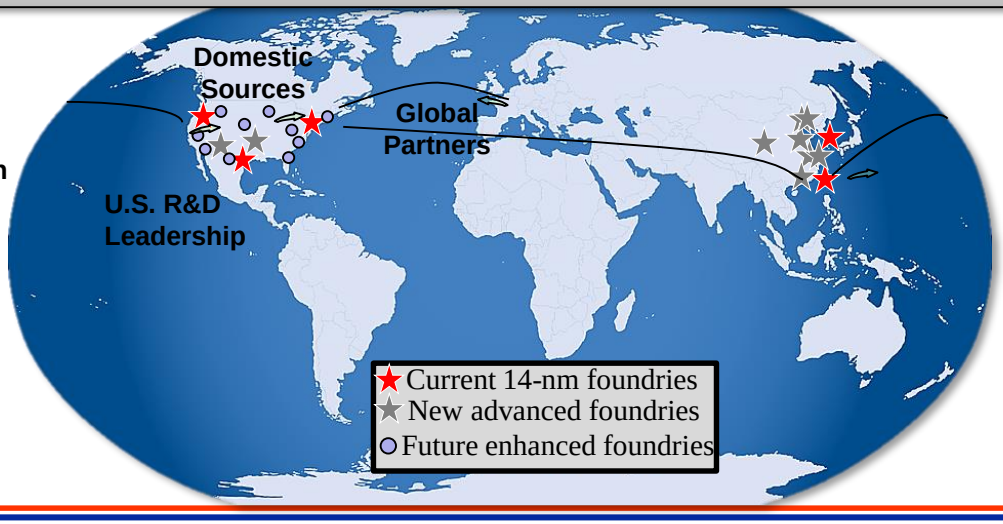
Current Global Microelectronics Leadership



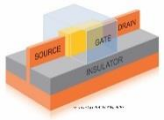


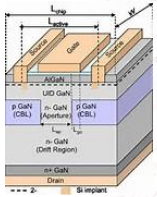
Possible Future Global Microelectronics Leadership





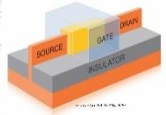
Create Microelectronics Innovation Throughout the United States



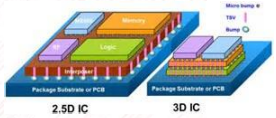


Fabrication Center

Innovation Hub



Design Center



Rebuilding US Microelectronics Leadership and Dominance

Strategic National Security Applications





Secure IoT

Financial & Data Analytics


Autonomous Systems + AI


Robust + Agile Communicators

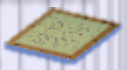

Commercial Space


Biomedical

Strategic National Economic Competitiveness Applications

Proactive Awareness & Security
- Supply Chain track
- Proactive Authorities
- Intelligence & CI

Access & Assurance
- Secure Design
- IP, EDA, experts
- Foundry assured Access
- Prototype Demonstrations



Enabling Manufacturing
- SoP Back-end parity with SotA
- SotA on 200mm tools at SoP
- Mini fabrication for high-mix low vol.

Incentives & Market Growth
- Acquisition reform & incentives
- Tax, policy, regulation reform
- R&D and domestic fab incentives

Strategic Alliances
- Cooperative R&D
- Trade & FMS
- Americas
- Europe
- Asia partners

Disruptive Research & Development

Materials, devices, circuits | Architectures | Design tools for Complexity

Experts, Infrastructure, Venture Capital | Science & Technology, R&D

Microelectronics Strategy Challenges & Investments

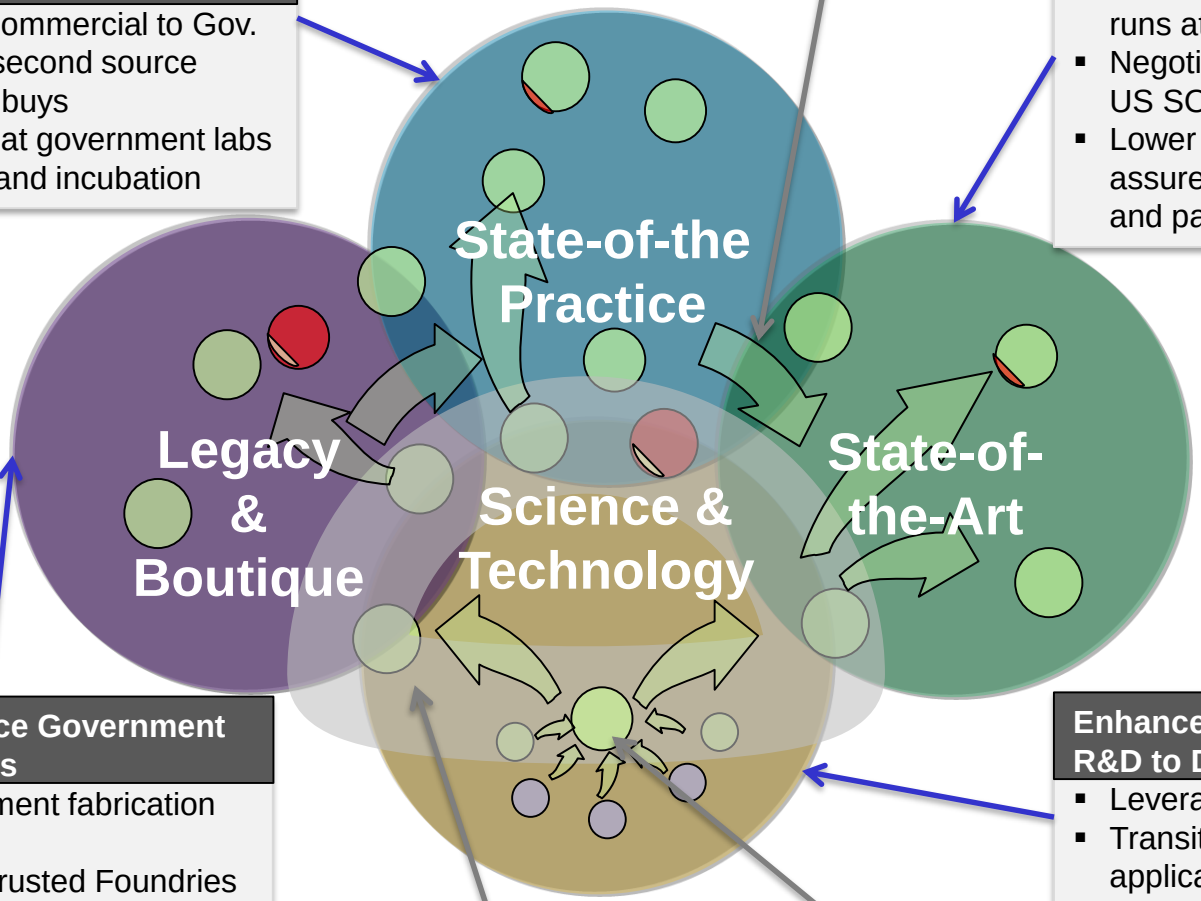
Preserving US Government Involvement in SoP

- IP transfer from commercial to Gov. and commercial second source
- Execute Lifetime buys
- Dual use-access at government labs for R&D capture and incubation

Enabling Manufacturing

Access to Assured SOTA in US

- Contract for access and shuttle runs at SOTA foundries
- Negotiate dedicated line(s) in a US SOTA foundry
- Lower barriers to innovation assured design, IP, fabrication and packaging



- **Commercial Access**
- **Commercial & Assured Gov. Line**
- **Government dual use**
- **R&D facilities**

Preserve & Enhance Government Unique Capabilities

- Enhance government fabrication capabilities
- Cooperate with Trusted Foundries for strategic radiation-hard
- Invest in development of disruptive fabrication tools for low-volume

Enhance and Bridge Disruptive R&D to Domestic Production

- Leverage and focus R&D
- Transition R&D capabilities to applications & production
- Invest in advanced materials, device, circuits, and complex systems design tools

Demonstrating Innovation for National Security and Interests

Innovators & Developers

Small Business, Individuals, defense and commercial R&D, FFRDCs, University researchers, etc.

Private | Gov.

Competitive Selection

Contest

Autonomy, IoT, Space, Bio, etc.

Judges

Gov. & Private Investors

Prototype Co-Development

A | **6.3-4**

Design Team, IP, Business Model, Demo Plan

$$ + services

Production & Adoption

B

Innovative Demo + Business Model + Customers

$$$

C

Market Tested Part + Business Model + Market

$$$$

Acquisitions

Risk Reduction + Side-car demo

$$$$

Maintenance

Refresh & Upgrade Ideas

$$$

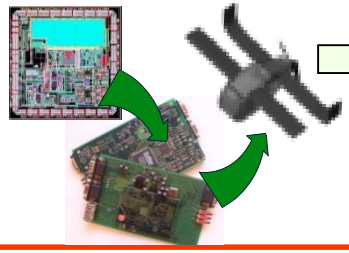
Adopters & Improvers

Contractors, Acquisition, private users, operators, and consumers

Private | Gov.

Communities, Infrastructure, & Investments

Designers, Innovators, VC, R&D, Gov. & Private	Secure EDA, 3rd & Gov. IP, V&V, Software, Simulators	Foundry Access, Packaging, Testing, etc.	Sponsors, Venture Capitol, Acquisition



Disrupting Innovation for National Security and Interests

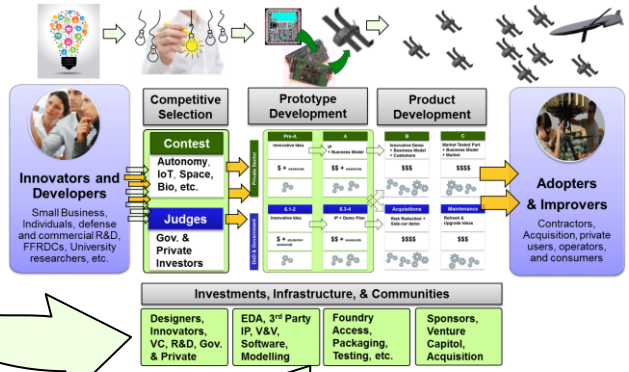
Enabling Ubiquitous Low-cost Manufacturing

90nm to 65nm & Copper
- Bring Gov. & merchant SoP to 65nm feature size with wet 193 litho
- Copper back end parity with SotA

SotA at SoP & Ebeam litho
- Multi-beam e-beam direct write litho for low-volume
- 200mm tools for SotA at SoP foundries

SotA Mini Fabs
- Plethora of miniature fabs for high-mix low-volume production
- Market for fab recipes & low-cost mini-fabs

Prototype Demonstrations



Disruptive Research and Development

Science & Technology R&D

Defense and commercial R&D, FFRDCs, University researchers, etc.

Materials & Devices
- Novel materials systems for next generation logic, memory, and interconnects
- Integrate novel devices with advanced SOTA microelectronics
- Demonstrate new circuits applications

Architectures
- Combine memory and processing on a single part
- Stackable, 3-D logic and memory
- Combine non-silicon and silicon components
- Calculations with new type of logic devices

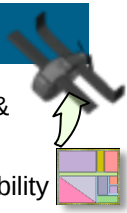
Complex Design
- Robust Software Development tools
- EDA tools to design complex systems with small agile teams

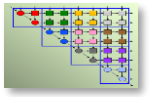
Innovators and Prototype Developers

Small Business, Individuals, defense and commercial R&D, FFRDCs, University researchers, etc.

Microelectronics Innovation for National Security

	Problem	Actions & Investments	Outcomes
Access & Assure Ecosystem	• **Few domestic SotA foundries** & packaging, dominated by commercial forces, **$$ to access**, growth in Asia • **Development complexity, costs**, and lack of expertise and security are stifling innovation in SoC ASIC hardware • DoD influence is limited & national **security needs not being met**	• Provide **Assured access** to SotA, SoP, and Gov. foundries & packaging • Provide **Assured development community** (IP, EDA, experts, secure computing, Gov. IP) for innovation • Support **Innovative co-development of 10-1000x capabilities** for USG and strategic growth application areas	• Strong **domestic assured source** for Gov. & private innovative microelectronics products • Significantly **reduced barriers** to rapid capability development with assurance for Gov. and cooperative emerging industries • Immediate **demonstration of 10-1000x** perf. for USG & industry in autonomous systems, IoT, financial, commercial space, etc.
Enabling Domestic Manufacturing	• Many domestic SoP foundries are at 200mm and >65nm nodes and **aren't being updated** • Advanced-node flexible, scalable manufacturing is **not available in U.S.** • **Innovative R&D going to foreign sources** to scale and integrate new device and circuits architectures	• **Enhance SoP foundries** to 65nm & copper back end & E-Beam litho now • Co-develop **advanced fabrication** (5-65nm) tools for existing 200mm • Develop mini-fab to **transform and distribute SotA** disruptive technology development for high-mix low-volume production	• Immediate **performance improvement** and close parity to SotA processes for USG purposes • Create **manifold sources** for SotA in the installed US SoP foundries to remain competitive • **Rapid low-cost development** of materials, device, and process for low cost high-mix and low-volume production to **capture innovation & manufacturing** throughout the U.S.
Dominate & Disrupt R&D	• USG investment in disruptive R&D for next- generation microelectronics has **significantly diminished** • **Research is stagnant** when an inflection point in the electronics industry marked by changes in Moore's Law is about to occur • The country that exploits this inflection point will maintain or obtain **economic and security superiority**	• Leverage DARPA JUMP program and industry collaboration to **develop disruptive materials & electronics** • Lead the development of **new circuit architectures** for next-generation computing and strategic applications • Develop tools and technologies that allow **rapid redesign of complex systems**	• Develop the onshore manufacturing and design capacity to **own the next generation** of microelectronics technology • Maintain **U.S. leadership** in the semiconductor industry with healthy **U.S. R&D community** • Highly **productive designers** able to develop **complex systems with assurance**, at a rapid pace and **low cost** to keep ahead of our global competitors





Systems Engineering: Critical to Defense Acquisition










Defense Innovation Marketplace
http://www.defenseinnovationmarketplace.mil

DASD, Systems Engineering
http://www.acq.osd.mil/se

For Additional Information

Dr. Jeremy Muldavin

ODASD, Systems Engineering

571-372-6690

jeremy.b.muldavin.civ@mail.mil

Backup

Commercial Computing Trends

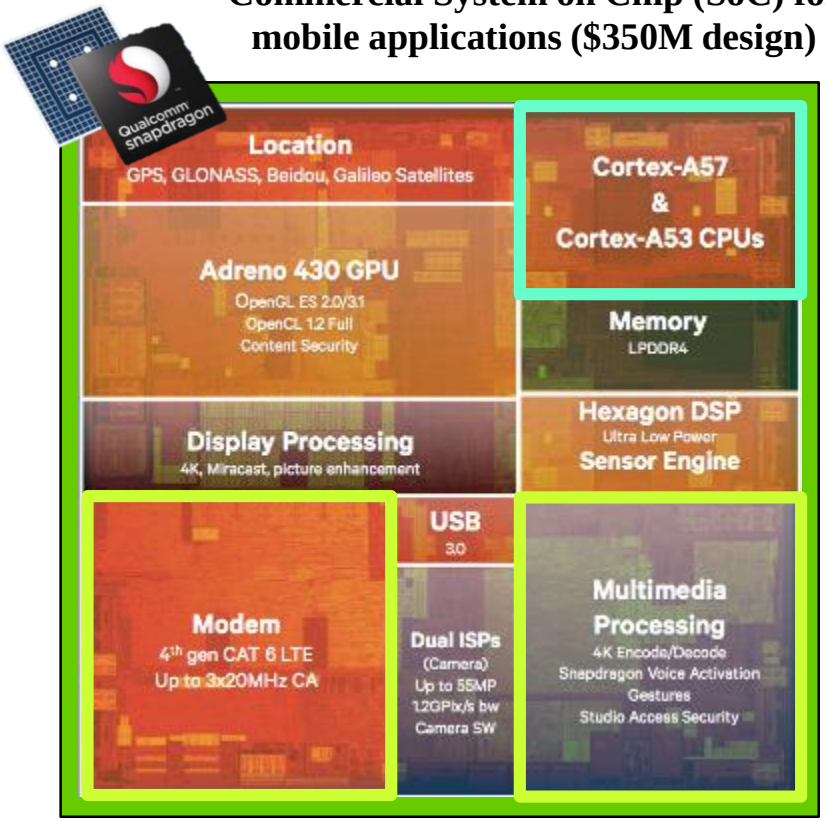
Mobile Computing

Internet of Things & SDR

Powerful Test & Measurement

Cloud Computing & Infrastructure

Commercial System on Chip (SoC) for mobile applications ($350M design)



Global mobile computing & infrastructure brings powerful capabilities to EVERYONE

Accelerators enable 10-1000x capabilities in SoC and server architectures

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

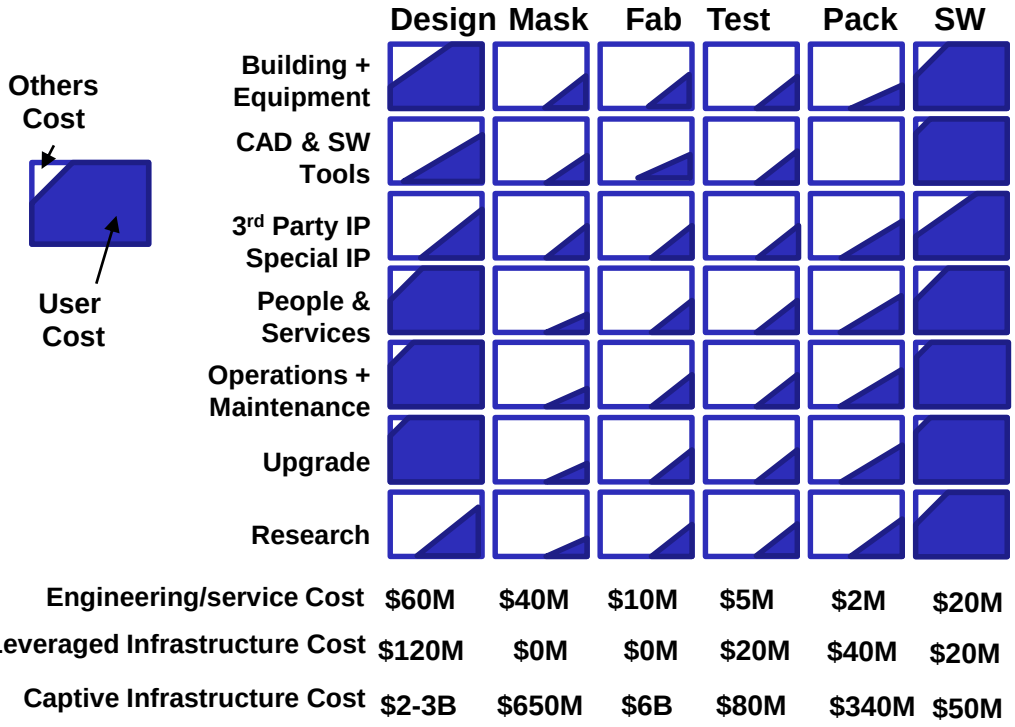
Preparation activities

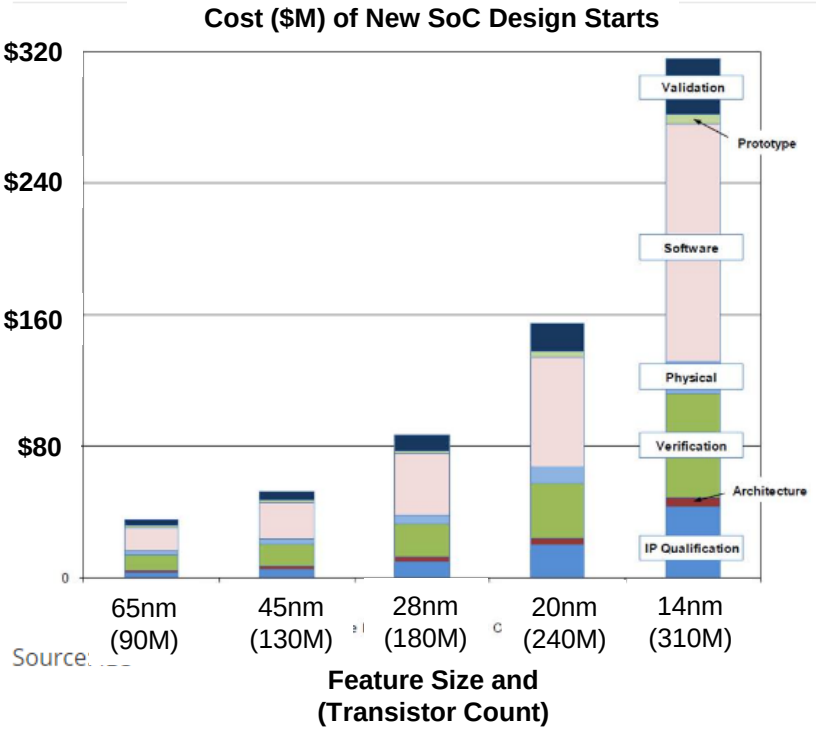
Capability development and demonstration

Deploy new capabilities

2015 2016 2017 2018 2019 2020 2021 2020 2023 2024

Barriers to Innovation Using (28nm) System on Chip

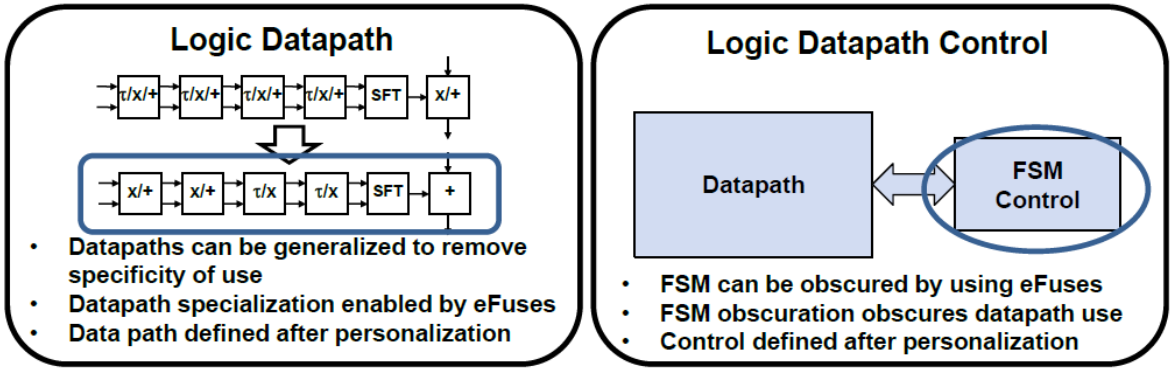




http://semiengineering.com/how-much-will-that-chip-cost/

Mitigations to Cyber Exploits of HW Vulnerabilities

- **Address Space Layout Randomization (ASLR)**
  - Randomly assigns memory layout to increase complexity of attack on specific memory locations
  - Using this method at runtime increases level of security
- **Obfuscation**
  - Multiple variants of HW to obfuscate circuit functionality against attacks
  - Data-path generalization to remove specificity of use



Reference:<http://www.darpa.mil/attachments/NDIA2.3.pdf>

Reference:<http://www.cs.vu.nl/~herbertb/download/papers/anc_ndss17.pdf>