Long-Term Strategy for DoD Trusted and Assured Microelectronics Needs

Jeremy Muldavin

Office of the Deputy Assistant Secretary of Defense for Systems Engineering

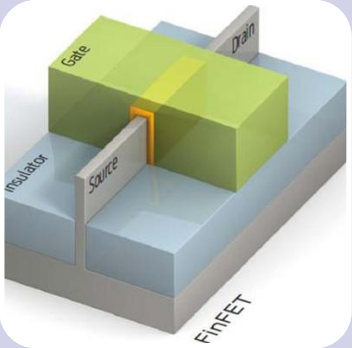
19th Annual NDIA Systems Engineering Conference

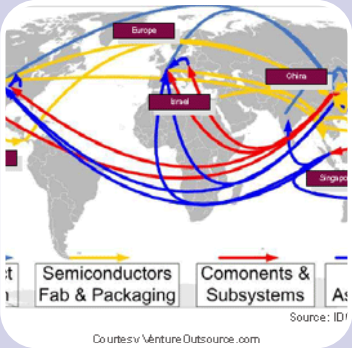
Springfield, VA | October 26 2016

Outline

- **State of advanced microelectronics for DoD applications**
- **Strategy to assure access for the DoD**
  - Need access to state-of-the-art integrated circuits (ICs) while maintaining an acceptable level of risk
  - New Trust and Assurance approaches to expand fabrication access
  - We want to maintain the U.S. technological and competitive edge in microelectronics
- **Partnership opportunities**
- **Questions**

Microelectronics Trends





State-of-the-art Devices

- Deeply-Scaled Silicon ICs (14nm)
- 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)

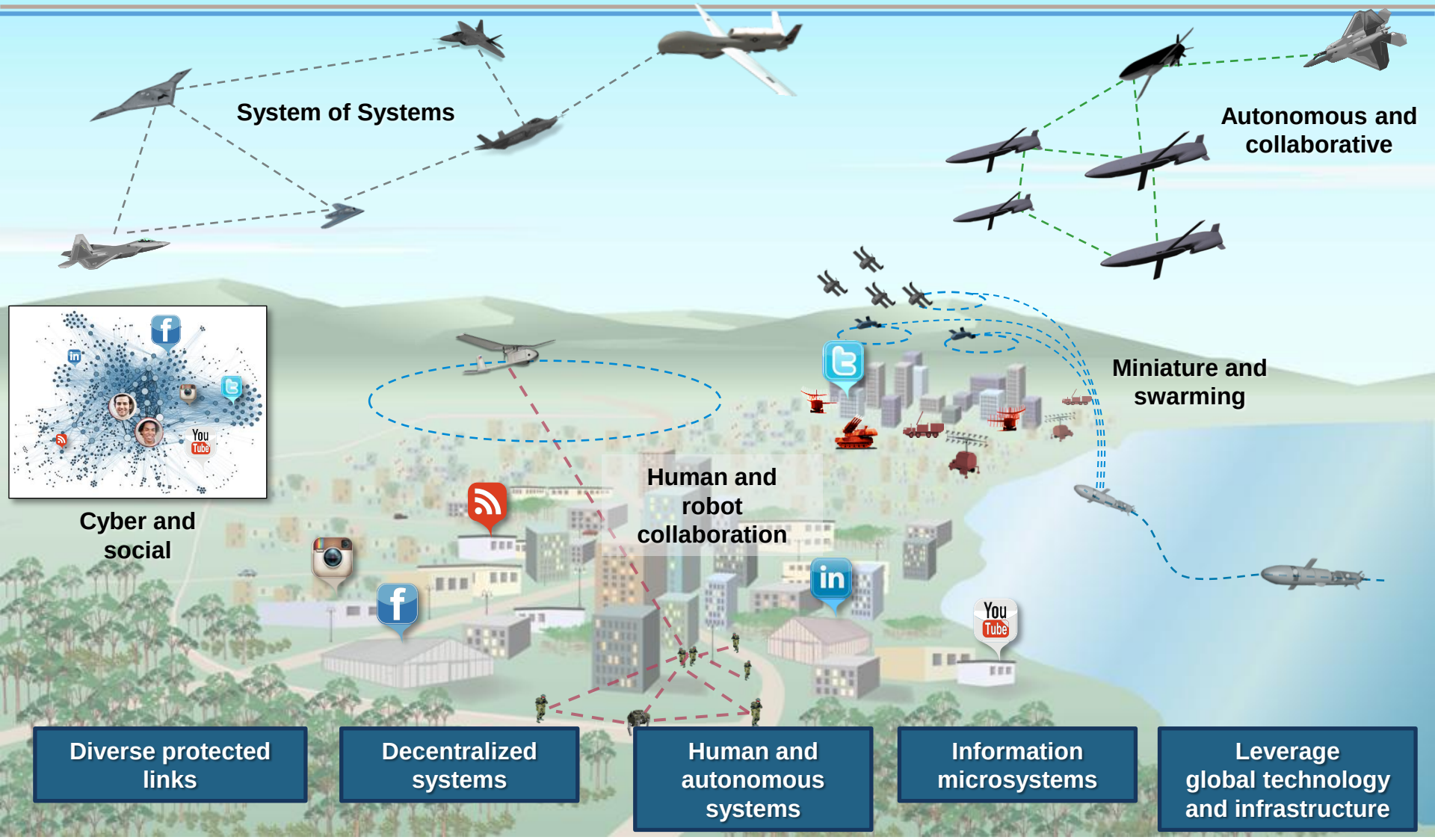
Globalization and Commercial Dominance

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

New Applications

- Internet of Things
- Big Data systems
- Autonomous systems
- Spectral and spatial communication agility

Future Warfighting Systems



Needs for Innovation in DoD Computing

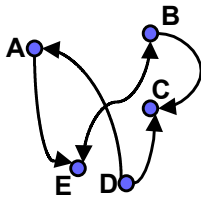
Challenges

- Parallelism and reduced efficiency of CPUs
- High cost and acquisition time
- Flexibility and sustainment for DoD applications
- Security and trust in global environment

Needs

Big Data and small platforms

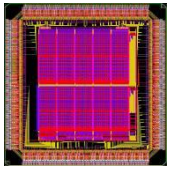
Artificial Intelligence (AI) and Graph Processors

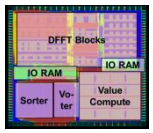


Forward Deployed PED and Miniature Sensor Systems

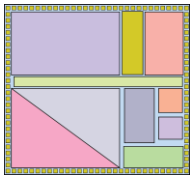
Contested environment computing

High Dynamic Range Flexible Radios and Digital Equalization





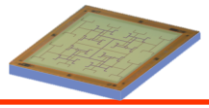
Heterogeneous SoCs



Systems of Systems and autonomy

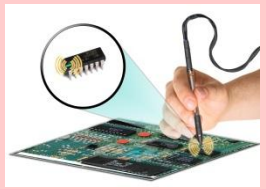
Autonomy Open Architecture

Vision and Precision Navigation and Timing (PNT) processing Application Specific Integrated Circuits (ASICs)



Cyber Protection and security

Assurance and Supply Chain Integrity

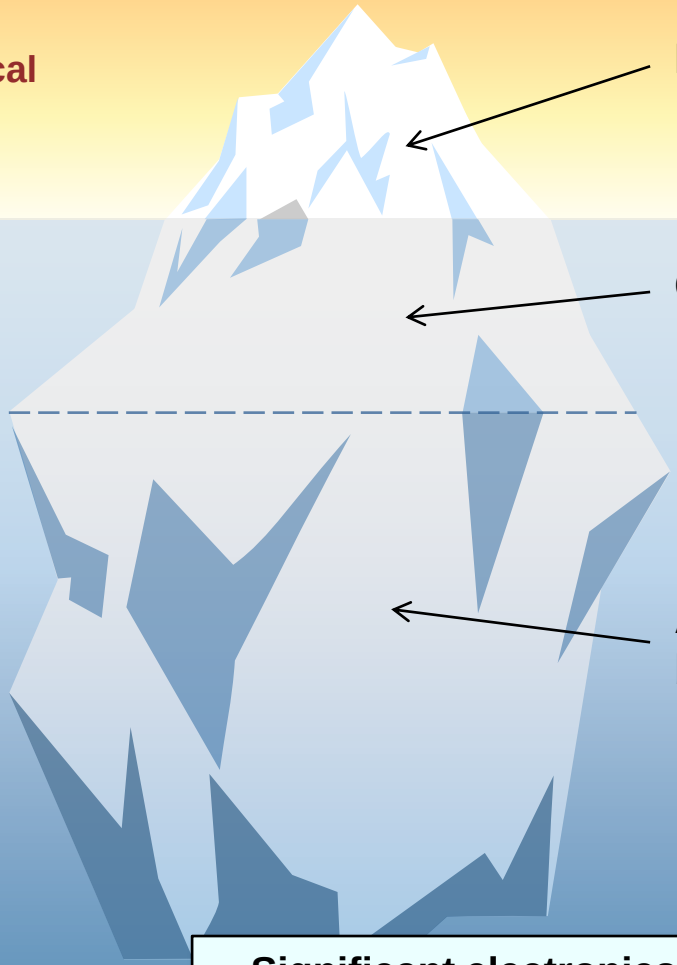


Cryptographic Key Management

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

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.

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

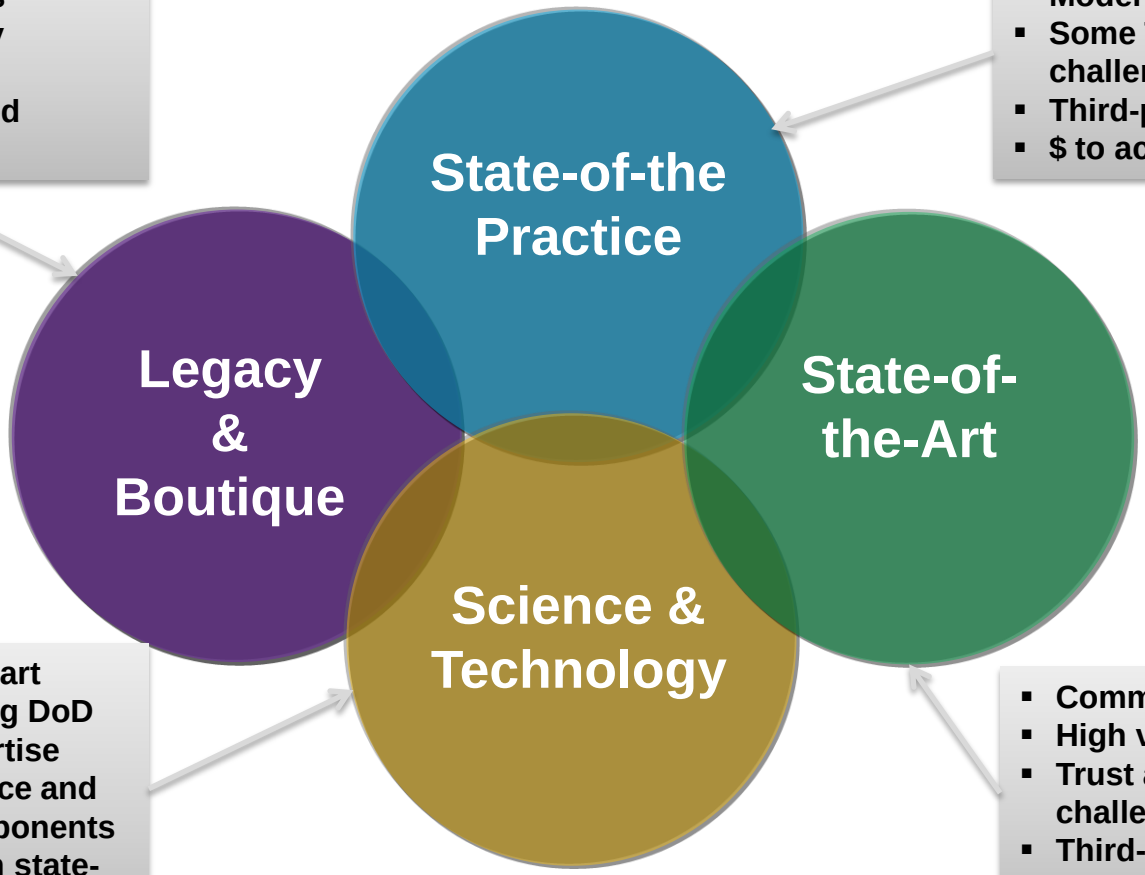
Significant electronics challenges represent a strategic level national issue

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

Microelectronics Strategy Challenges

- DoD-driven
- Availability concerns
- Yield and complexity challenges
- Specialized IP needed
- $$ to maintain

- Commercially-driven
- Moderate volumes required
- Some Trust and assurance challenges
- Third-party IP necessary
- $ to access



- Follows state-of-the-art (offshore) threatening DoD Subject Matter Expertise
- Investing in assurance and beyond-Silicon components
- Long-term impact on state-of-the-art

- Commercially-driven
- High volumes desired
- Trust and assurance challenges
- Third-party IP necessary
- $$$ to access

Four Distinct Interrelated Domains

DoD Microelectronics Goals

Access

- Lower barriers to safely access and develop advanced semiconductor-based systems to address new threats
- Robust design & validation tool availability

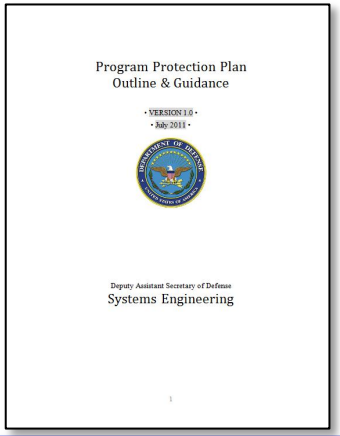
Assurance

- Leverage an assured global supply and partners in U.S. semiconductor industry
- Assurance as a competitive advantage for U.S. and Defense Industrial base

Boutique & Legacy

- Assured and expanded supply chain for specialized microelectronics for DoD systems
- Increased assurance and expanded supply options for Legacy parts

What We are Doing

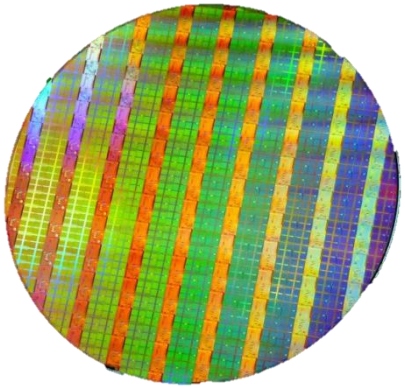


Policy

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

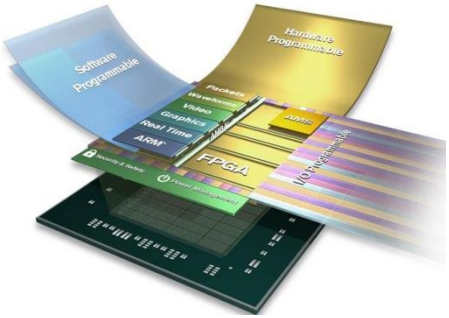
Joint Federated Assurance Center

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



Trusted & Assured Microelectronics

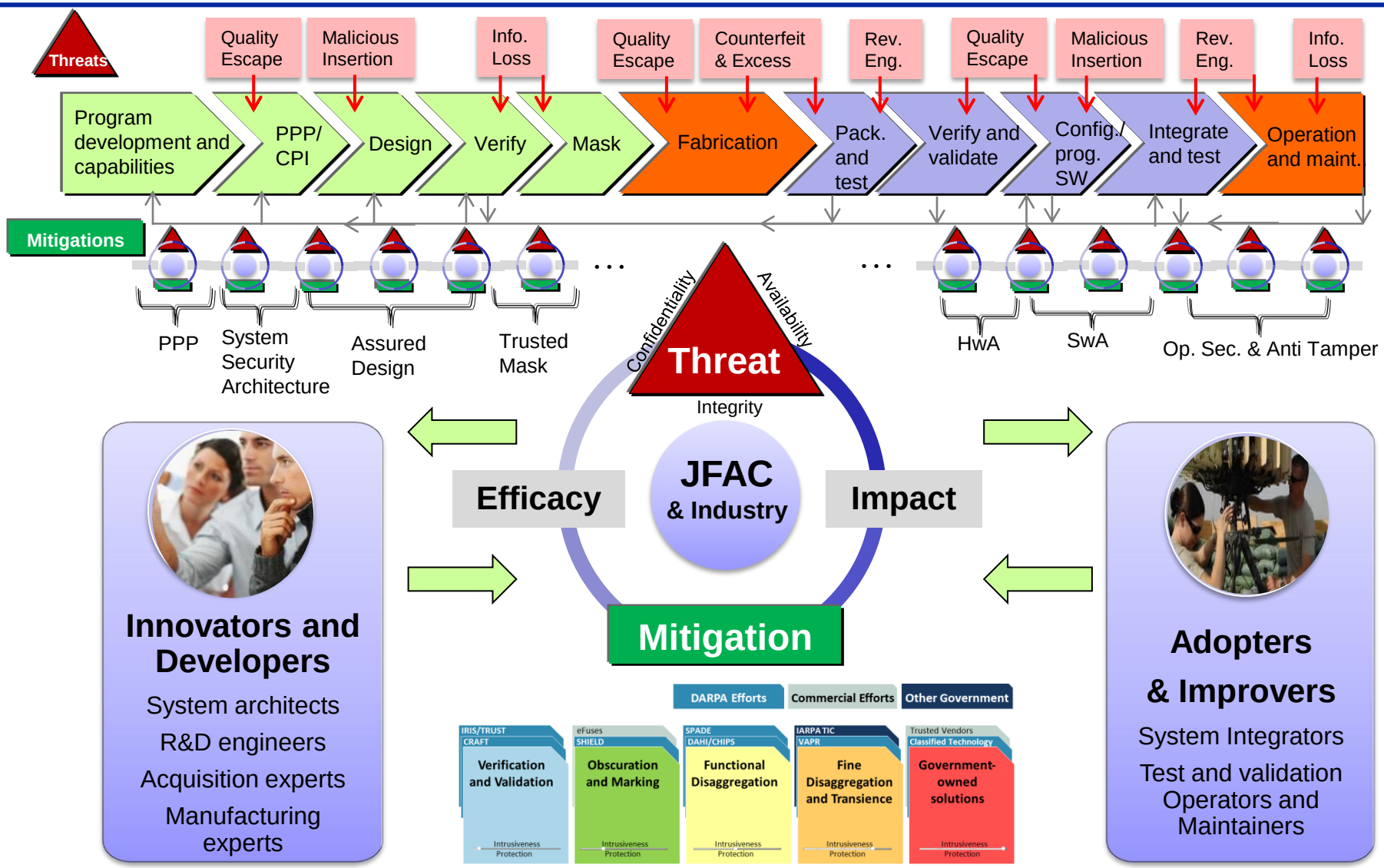
- Access to state-of-the-art foundries
- Trust and assurance methods and demonstration
- Industrial best practices for assurance



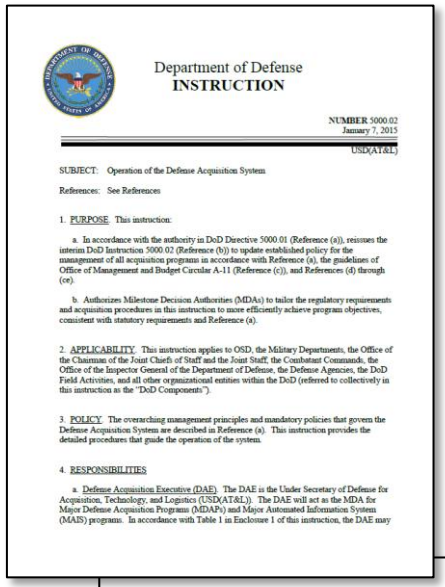
COTS and FGPA

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

Systems Engineering Approach



Program Protection Planning Policy



Department of Defense
INSTRUCTION

NUMBER 5000.02
January 7, 2015
USD(AT&L)

SUBJECT: Operation of the Defense Acquisition System

References: See References

1. PURPOSE. This instruction:

a. In accordance with the authority in DoD Directive 5000.01 (Reference (a)), reissues the interim DoD Instruction 5000.02 (Reference (b)) to update established policy for the management of all acquisition programs in accordance with Reference (a), the guidelines of Office of Management and Budget Circular A-11 (Reference (c)), and References (d) through (ce).

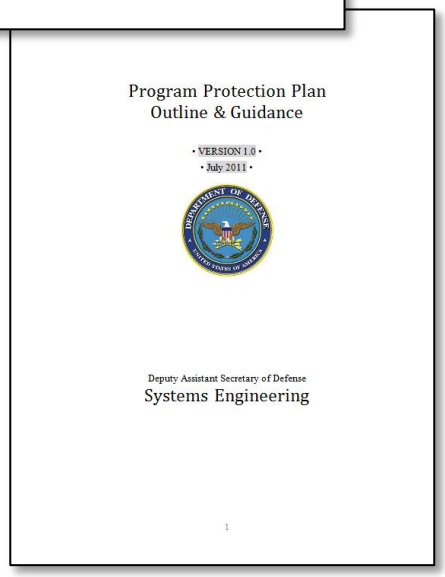
b. Authorizes Milestone Decision Authorities (MDAs) to tailor the regulatory requirements and acquisition procedures in this instruction to more efficiently achieve program objectives, consistent with statutory requirements and Reference (a).

2. APPLICABILITY. This instruction applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this instruction as the "DoD Components").

3. POLICY. The overarching management principles and mandatory policies that govern the Defense Acquisition System are described in Reference (a). This instruction provides the detailed procedures that guide the operation of the system.

4. RESPONSIBILITIES

a. Defense Acquisition Executive (DAE). The DAE is the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)). The DAE will act as the MDA for Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) programs. In accordance with Table 1 in Enclosure 1 of this instruction, the DAE may



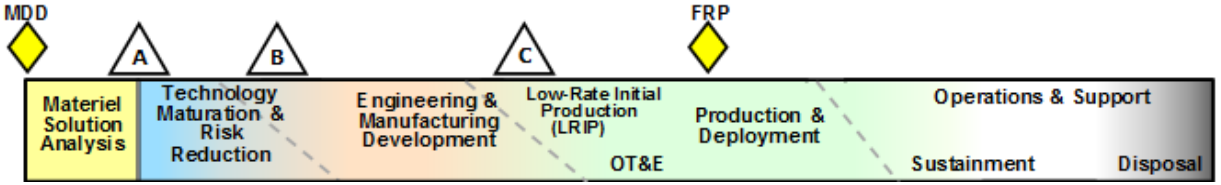
Program Protection Plan
Outline & Guidance

• VERSION 1.0 •
• July 2011 •

Deputy Assistant Secretary of Defense
Systems Engineering

1

- **System Security Engineering is accomplished in the DoD through PPP**
- **DoDI 5000.02 requires program managers to employ system security engineering practices and prepare a PPP to manage the security risks to Critical Program Information, mission-critical functions and information**
- **Program managers will describe in their PPP:**
  - Critical Program Information, mission-critical functions and critical components, and information security threats and vulnerabilities
  - Plans to apply countermeasures to mitigate associated risks:
    - Supply Chain Risk Management
    - Hardware and software assurance
  - Plans for exportability and potential foreign involvement
  - The Cybersecurity Strategy and Anti-Tamper plan are included



Trusted Foundry Long-Term Strategy

Program goals:

- Protect microelectronic designs and IP from espionage and manipulation
- Advance DoD hardware analysis capability and commercial design standards, e.g., physical, functional, and design verification and validation
- Mature and transition new microelectronics trust model that leverages commercial state-of-the-art capabilities and ensures future access

Technical challenges:

- Develop alternate trusted photomask capability to preserve long-term trusted access and protection of IP
- Scale/enhance the government's ability to detect security flaws in ICs
- Leverage academic and industry research for assuring trust from any supplier

Program partners:

- DoD science & technology (S&T), acquisition communities, academia, and industry

Provides technical solutions that can be leveraged by government and industry to enable microelectronics assurance

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

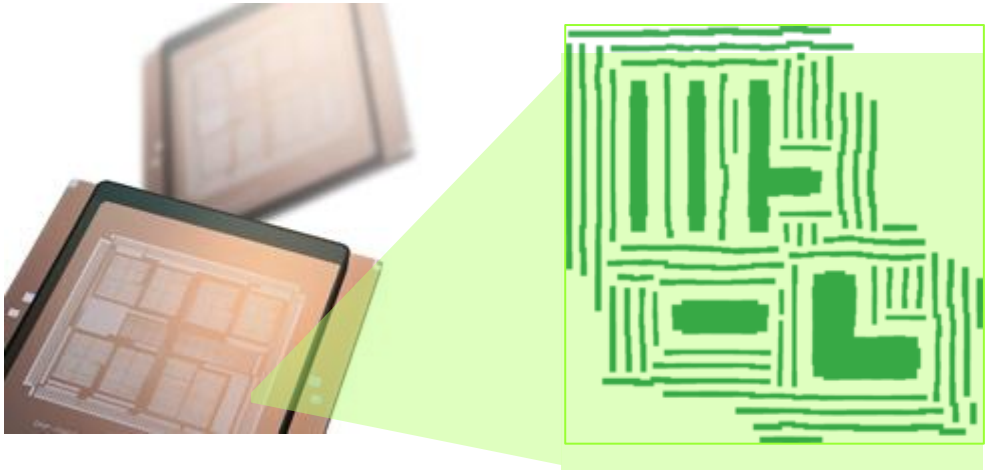
Advanced Technology and Alternative Techniques for Microelectronics Hardware Trust

Preparation activities | Capability development and demonstration → Deploy new capabilities

2015 2016 2017 2018 2019 2020 2021 2022 2023 2024

Alternate Source for Trusted Photomasks

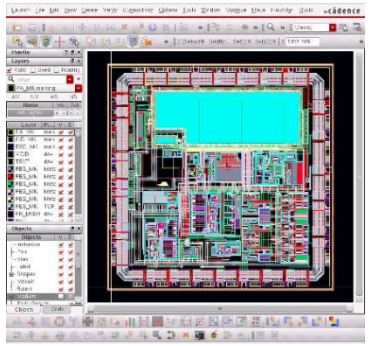
- **Develop second leading-edge Trusted photomask shop**
  - Trusted flow in data preparation and manufacturing designs needed to manage risk of IP theft and malicious alteration
  - GlobalFoundries currently only source of Trusted leading-edge masks
  - A second leading-edge source will ensure tape-in/mask release, mask manufacturing, and authentication process
  - Goal is to have secure, SECRET-level capabilities with a photomask supplier who has business relationships with leading-edge foundries

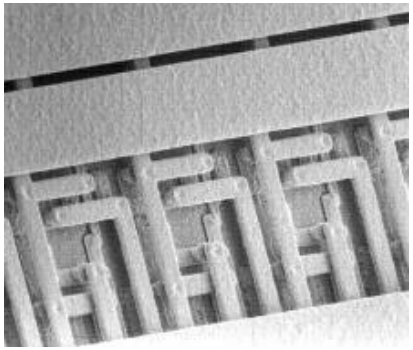


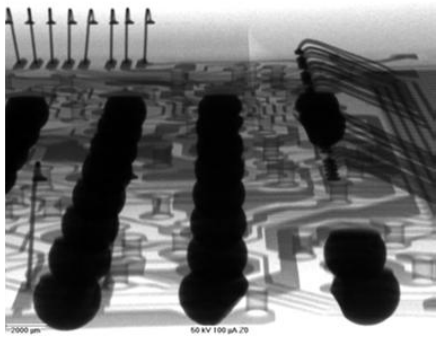
Microelectronics Trust Verification Technologies

- **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







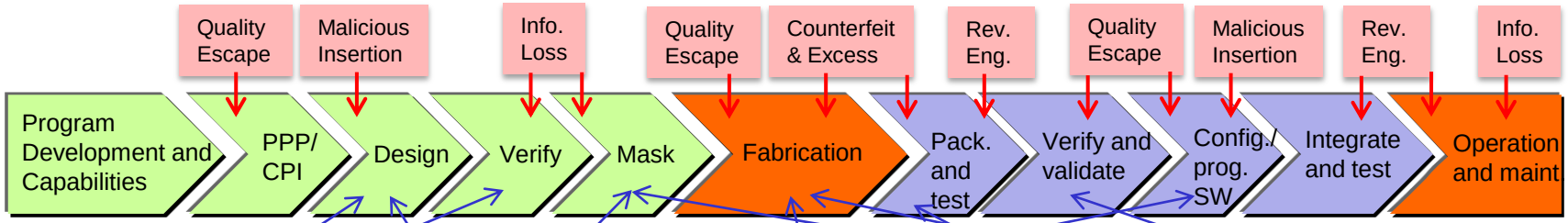
DoD, Intelligence Community, and DoE enhancing capability to meet future demand

Microelectronics Assurance Industrial Best Practices

- **Need industry-wide standards for assurance and security throughout the microelectronics supply chain**
  - Leverage efforts by the electronic design automation (EDA), manufacturer, integrator, and other vendor communities to develop security in an open architecture
  - Use government, industry, and academic threat and vulnerability resources to ensure security being developed is adequate for the threat
  - Who else should care about this?
    - Bio-tech community
    - Autonomy and AI community
    - Internet of Things and cloud computing providers
  - What are the benefits?
    - DoD leverages rapid innovation, ability to upgrade, and adapt to threats
    - Assurance for consumers through tracking, authentication, observability, etc., for next generation systems

Assurance as a competitive advantage in new markets

Advanced Technology and Alternative Techniques for Trust & Assurance



Design for trust

- Designing techniques to limit full use/functionality to trusted operation

IP protection

- Preventing exploitation, including control of use, concealment, reconfiguring, partitioning, or employment

Low-volume/high-mix production

- Innovative methods to permit cost-effective, Trusted and assured low volume manufacturing of state-of-the-art ICs

Electronic component markers

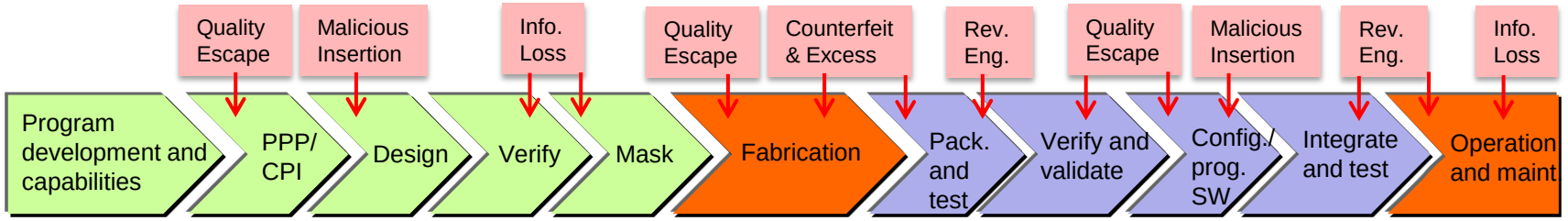
- Tagging/marking ICs and subassemblies to authenticate and track supply chain movements

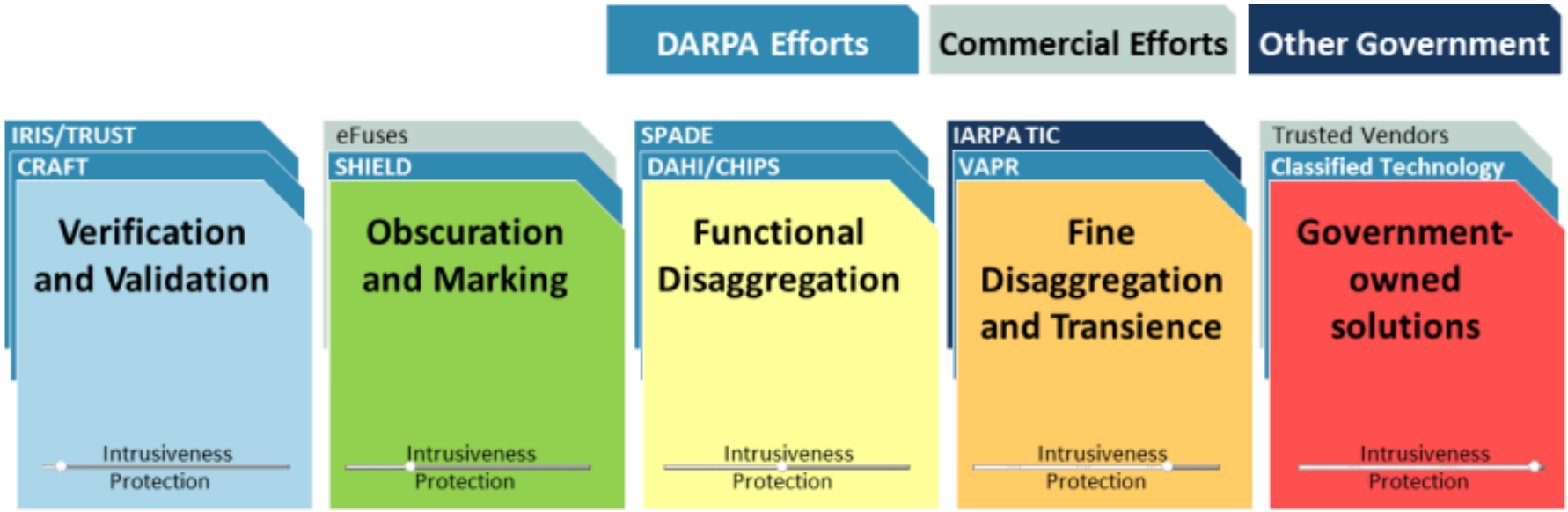
Imaging technologies and forensics

- Advanced capabilities to efficiently evaluate dense, state-of-the-art commercial components

Implement and demonstrate assurance capability with transition partners

Partner Efforts in Trust and Assurance

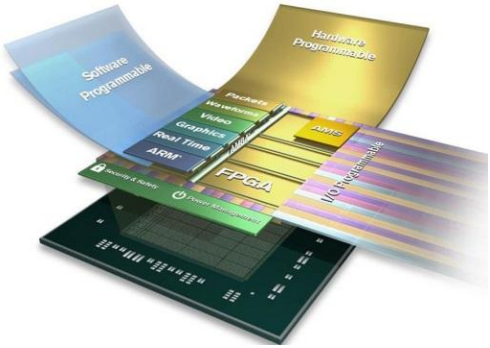




DARPA and IARPA are critical partners in development and transition

Assurance Strategy for FPGAs

- **FY 2016 goals for this effort:**
  - Produce a coherent, focused strategy/plan for FPGA assurance
    - Leverage existing USG and industry efforts to the maximum extent possible
    - Promote community awareness of related USG efforts via a series of workshops and conference calls sponsored by OASD(R&E), in coordination with the JFAC, National Security Agency (NSA), and Sandia National Laboratories (SNL)
    - As a community, identify the portfolio of related efforts on which we should focus with the goal of synchronizing and eliminating stove-pipes and separate, single-point solutions when possible
    - Identify gaps and/or activities requiring investment and elevate relevant needs to the JFAC Steering Committee (SC) for prioritization and direction regarding resourcing
      - In particular, align with, and inform, the execution plan for the Trusted Foundry Long-Term Strategy



Teaming and Partnerships are Key to Success

Many stakeholders are involved in the success of the long-term strategy:

- Leadership from OSD, Services, and agencies
- Performers including NSWC Crane, DMEA, DARPA, and other DoD S&T organizations and laboratories
- Integration and support of functions of:
  - DoD Trusted Foundry Program
  - DMEA Trusted Supplier Accreditation Program
  - JFAC
  - Microelectronics trust S&T and transition activities
- Coordination with other U.S. Government agency partners
- Building and leveraging partnerships with Defense and commercial industry and academia

Bottom line – structuring activities to meet acquisition program needs for trust and access to state-of-the-art microelectronics

The Way Ahead

- **Program engagement**
  - Foster early planning for HwA and SwA, design with security in mind
  - Implement expectations in plans and on contract
  - Support vulnerability analysis and mitigation needs
- **Community collaboration**
  - Achieve a networked capability to support DoD needs: shared practices, knowledgeable experts, and facilities to address malicious supply chain risk
- **Industry engagement**
  - Communicate strategy to tool developers
  - Develop standards for common articulation of vulnerabilities and weaknesses, capabilities and countermeasures
- **Advocate for R&D**
  - HwA and SwA tools and practices
  - Strategy for trusted microelectronics that evolves with the commercial sector
- **People!**
  - Improve awareness, expertise to design and deliver trusted systems

Systems Engineering: Critical to Defense Acquisition










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

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

Twitter: @DoDInnovation

BACKUPS

Trusted Foundry Program at DMEA

- **DMEA is responsible for assuring the access to microelectronics for critical DoD systems**

- **DoD Instruction 5200.44 requires that;**
  - *"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))."*

- **Holds Trusted Foundry licensing agreements (transferred from NSA) with ~70 foundries and suppliers**

- **Pursuing new Trust and Assurance accreditation instruments to broaden access and encourage industry best practices**

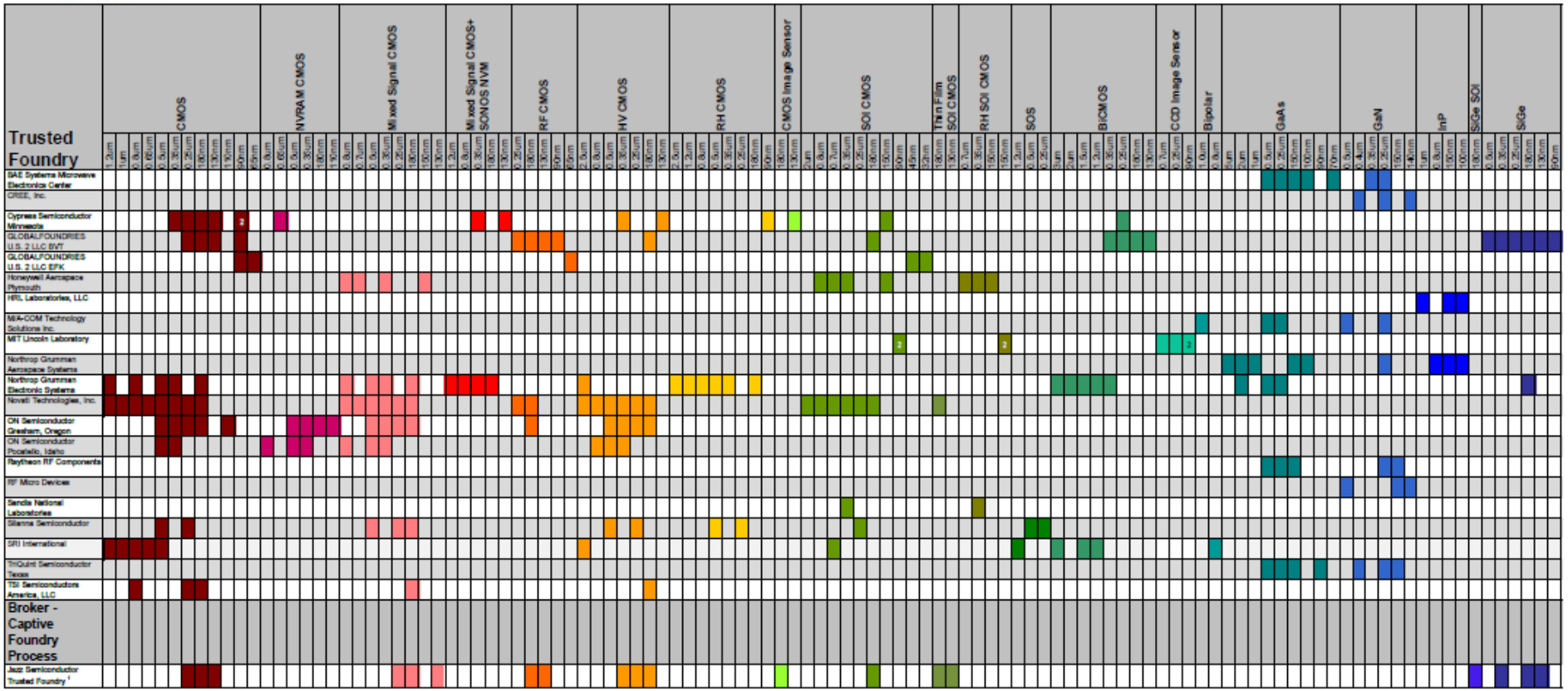
JFAC

- **JFAC is a federation of DoD SwA and HwA capabilities and capacities**
  - To support programs in addressing current and emerging threats and vulnerabilities
  - To facilitate collaboration across the Department and throughout the lifecycle of acquisition programs
  - To maximize use of available resources
  - To assess and recommend capability and capacity gaps to resource
- **Innovation of software and hardware inspection, detection, analysis, risk assessment, and remediation tools and techniques to mitigate risk of malicious insertion**
  - R&D is key component of JFAC operations
  - Focus on improving tools, techniques, and procedures for SwA and HwA to support programs
- **Federated Organizations**
  - Army, Navy, AF, NSA, DMEA DISA, NRO, and MDA laboratories and engineering support organizations; Intelligence Community and Department of Energy

The mission of JFAC is to support programs with SwA and HwA needs

Trusted Foundry Program at DMEA

- **Trusted Foundry program has broad participation and covers a wide range of semiconductor technologies and process nodes**



(http://www.dmea.osd.mil/otherdocs/AccreditedSuppliers.pdf)

Commercial Computing Trends

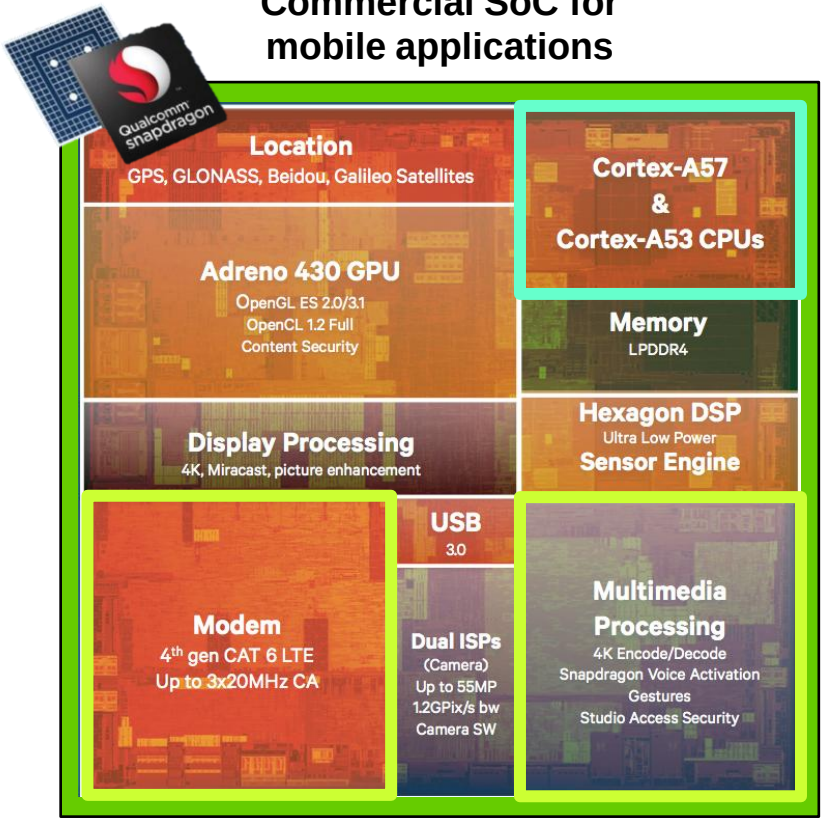
Mobile computing

Internet of Things and Software Defined Radio

Powerful test and measurement

Cloud computing and infrastructure

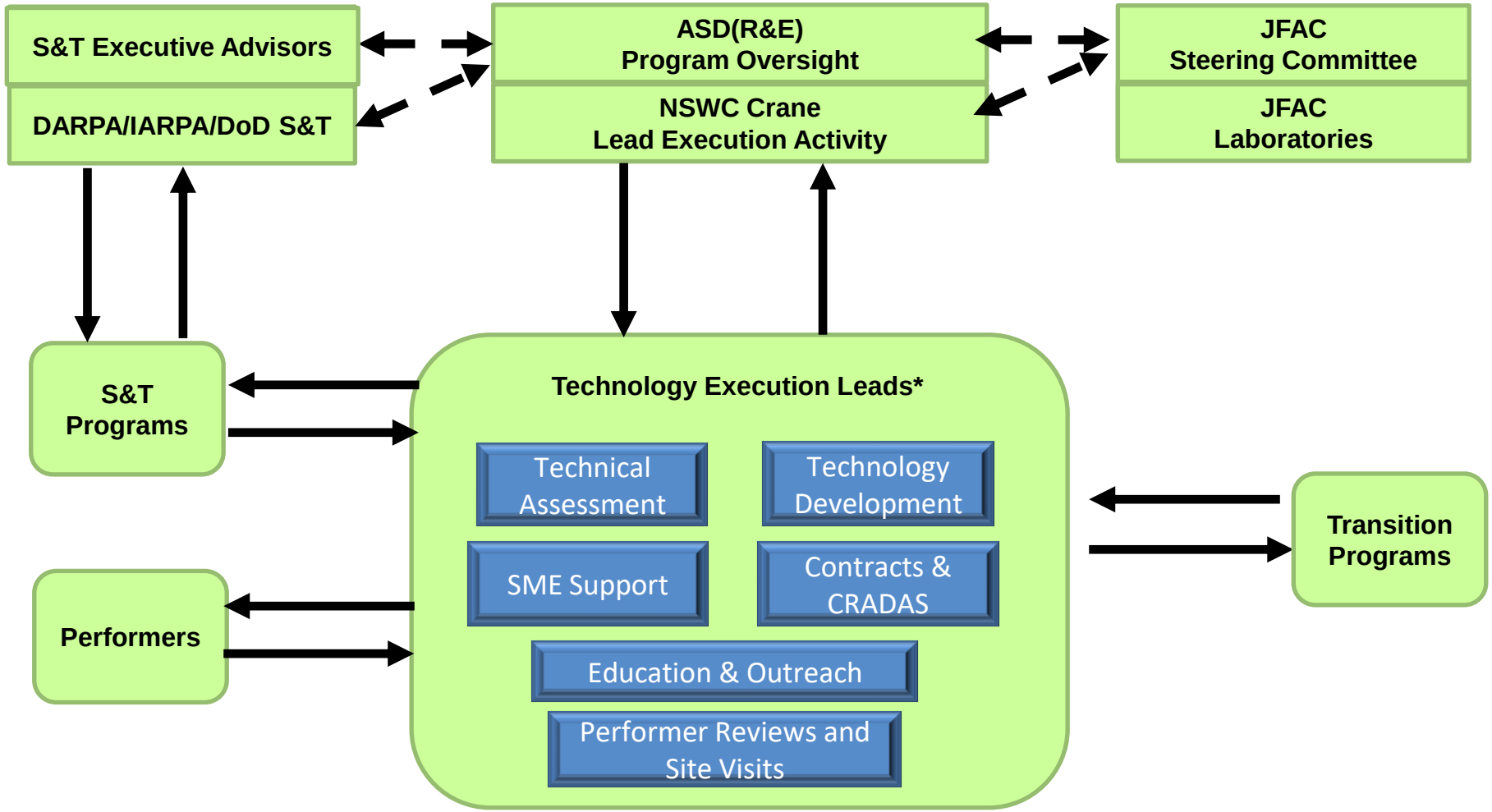
Commercial SoC for mobile applications



Global mobile computing and wireless infrastructure brings powerful capabilities to nearly everyone

SoCs with custom accelerators enable size, weight and power (SWaP)-efficient mobile applications and servers

Notional T&AM Management Model



**Based on JFAC Hardware Assurance Gap Analysis and Program Needs