IDA
Institute for Defense Analyses
4850 Mark Center Drive • Alexandria, Virginia 22311-1882

Hardware Assurance (HwA) Support for Supply Chain Risk Management (SCRM)

Brian S. Cohen
703-845-6684, bcohen@ida.org

Defense Standardization Program Workshop
July 10, 2018

This material represents ongoing technical work and the views of the author and does not necessarily represent any policies or positions of the government.

IDA

Purpose

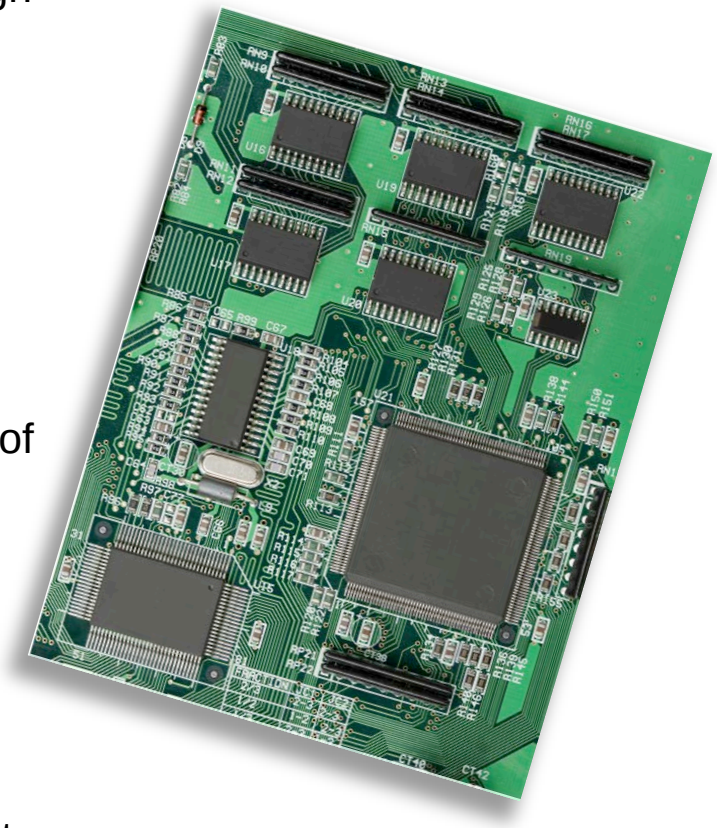
- Hardware Assurance addresses
  - Supports the government Supply Chain Risk Management (SCRM) activities for electronics hardware
  - Seeks to detect and prevent possible malicious activities in the supply chain
  - Seeks to detect vulnerabilities in electronic products
  - Provides expertise to government counterfeit prevention and detection activities
  - Informs standards, policy and guidance development

Definitions

- **Assurance** – The level of confidence that the system and its critical components function as intended through mitigation of known exploitable vulnerabilities and potential malicious insertions, and protection of IP throughout their lifecycle *(Proposed definition)*

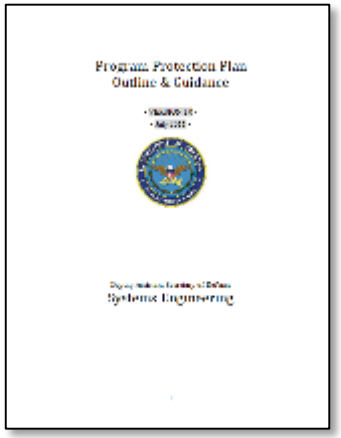
- **Critical Component** – A component which is or contains information and communication technology, including hardware, software, and firmware, whether custom, commercial, or otherwise developed, and which delivers or protects mission critical functionality of a system or which, because of the system's design, may introduce vulnerability to the mission critical functions of an applicable system *(Source: DoDI 5200.44)*

- **SCRM** – A systematic process for managing supply chain risk by identifying susceptibilities, vulnerabilities and threats throughout DoD's "supply chain" and developing mitigation strategies to combat those threats whether presented by the supplier, the supplied product and its subcomponents, or the supply chain (e.g., initial production, packaging, handling, storage, transport, mission operation, and disposal) *(Source: DoDI 5200.44)*



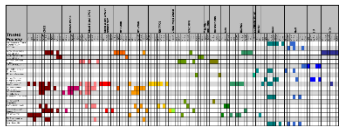
* A proposed definition

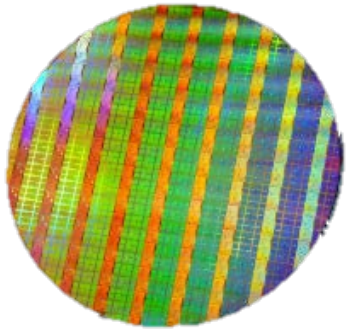
DoD Strategy and Actions

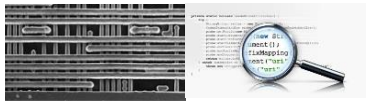


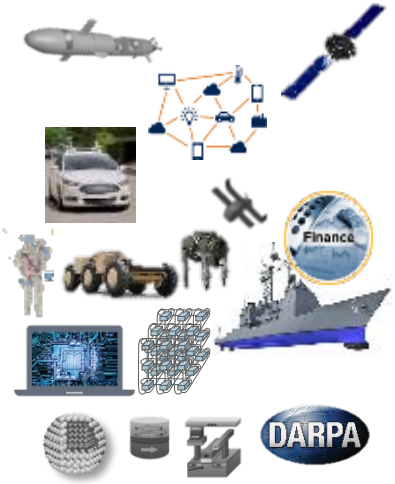
Trusted Supplier Accreditation

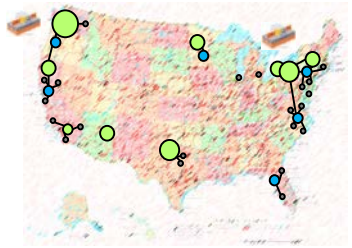
TAPO

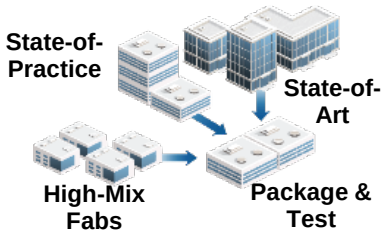












Policy

- Program Protection Plan (PPP), DoDI 5200.44, ITAR, DPA Title III
- Strategy/Directive for assured microelectronics
- National Security Strategy priority

DMEA

- Maintain and expand the number of trusted suppliers
- Provide access to state-of-the-art trusted flow (TAPO)
- Support sensitive needs and operations

Trusted & Assured Microelectronics

- Assured access to state-of-the-art foundries through modern trust and assurance methods and demonstration
- Industrial standards for assurance
- JFAC enhancement

DoD MINSEC

- Next generation DARPA ERI R&D captured in U.S.
- Modernization and assurance for DoD and nation through innovation ecosystems
- Radiation-hardened microelectronics for nuclear and space

Domestic Foundry & Packaging

- Multiple competitive state-of-the-art foundries on shore
- Leadership in R&D and production
- Strong commercial business models
- Government business model for innovation and assurance

Joint Federated Assurance Center (JFAC) Mission

IDA

The JFAC is a federation of DoD organizations that have a shared interest in promoting software and hardware assurance in defense acquisition programs, systems, and supporting activities. The JFAC member organizations and their technical service providers interact with program offices and other interested parties to provide software and hardware assurance expertise and support, to include vulnerability assessment, detection, analysis, and remediation services, and information about emerging threats and capabilities, software and hardware assessment tools and services, and best practices.

JFAC HwA Services

JFAC Service Providers deliver expert advice and help to Program Executive Offices (PEOs) and programs to "engineer-in assurance":

- Integrated circuit secure design and verification & validation (V&V)
- Criticality Analysis
- Milestone reviews
- Deployment assistance and review
- State-of-the-art HwA practices (i.e., USG, commercial industry, academia) for potential applied R&D opportunities
- HwA considerations for acquisition planning/RFP preparation
- Sampling strategies
- Comprehensive V&V strategies
- Red teaming
- Supply Chain Risk Management (SCRM)
- HwA-specific contracting language and deliverables
- Sustainment support
- Executing full spectrum of analysis (including possible destructive analysis) as per SAE Standard AS6171

- Counterfeit Detection
- Nondestructive Hardware Analysis
- Functional Analysis
- Hardware Authentication
- Trusted Foundry and Secure Chip/Board Fabrication
- Anti-tamper (AT)
- Incident Response and Forensic Analysis (HwA)
- Application-Specific Integrated Circuit (ASIC) / Field-Programmable Gate Array (FPGA) Verification
- Secure Design
- Failure and Material Analysis
- Firmware Security Analysis

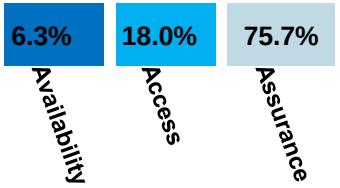
DoD Trusted & Assured Microelectronics (T&AM) FY18 Activities and Investments

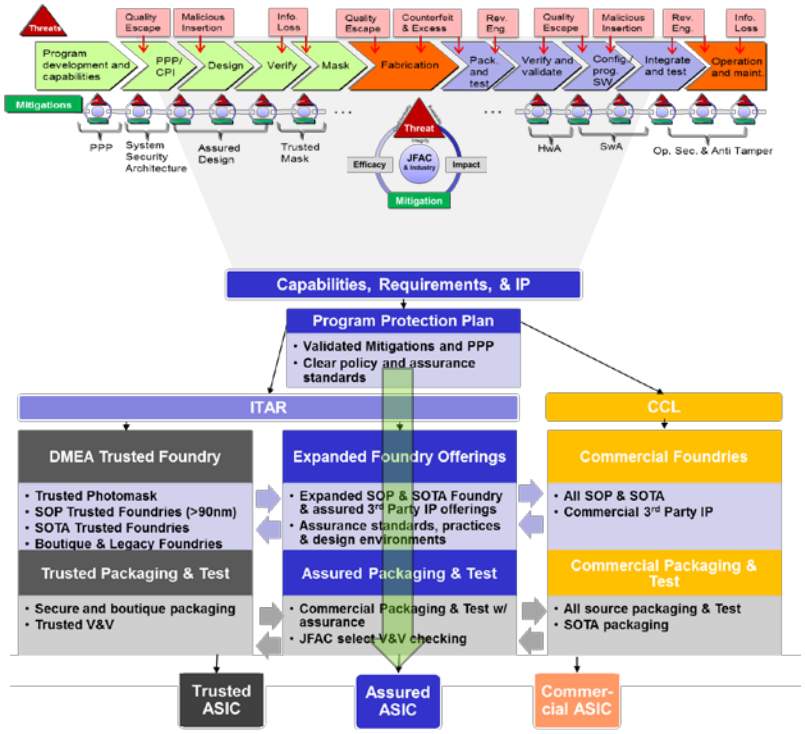
IDA

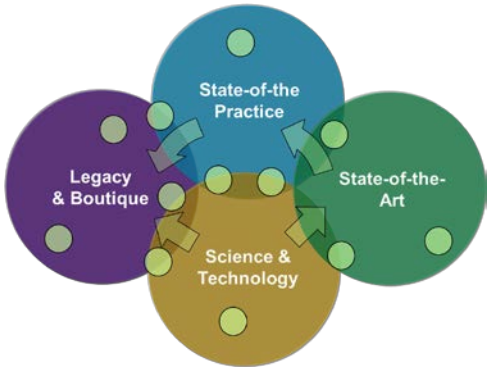
Overall

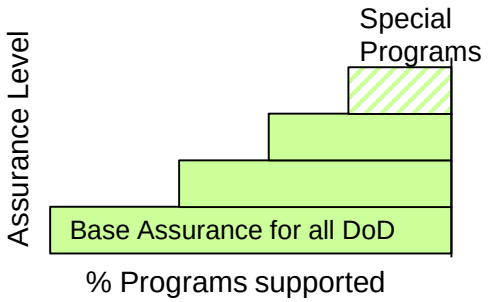
Inputs	Investments & Actions	Deliverables & Outcomes
• Government, e.g., DARPA, IARPA, and commercial assurance technologies • JFAC labs, DMEA, FFRDCs • DoD programs and commercial suppliers	• <u>Develop, mature and demonstrate</u> assurance mitigations • Evaluate effectiveness of protections of IP and integrity • Support trusted mask fabrication • Transition to, and support of, 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



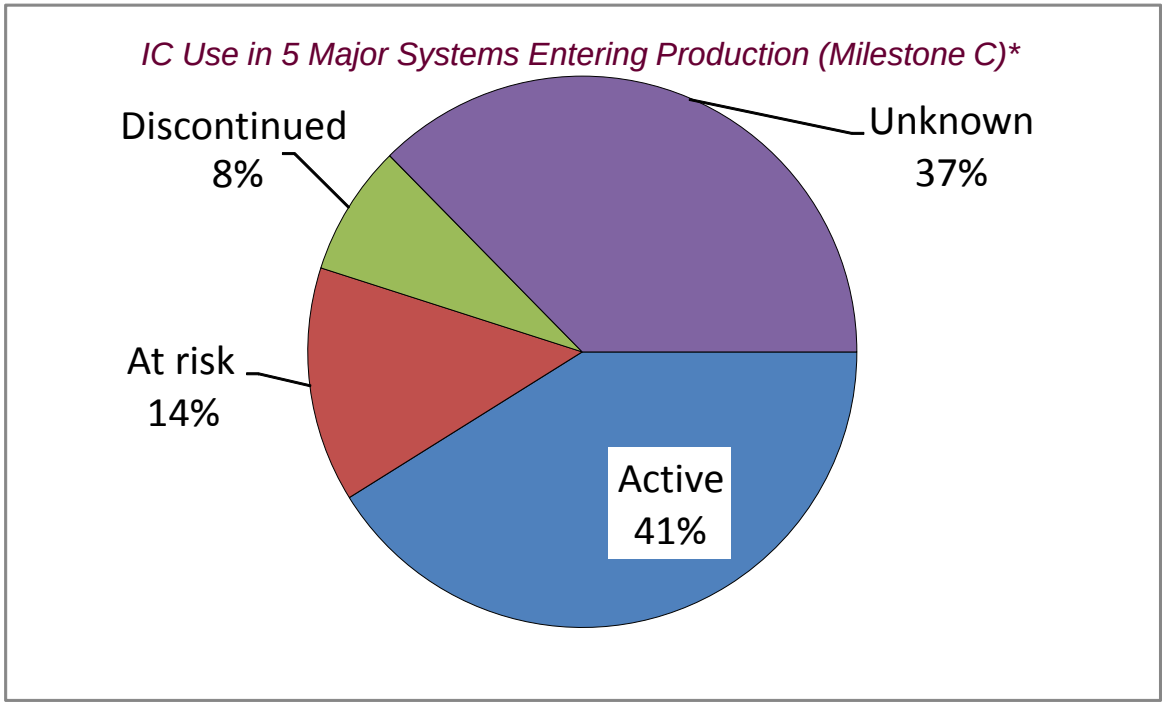






Microelectronics Obsolescence Risk

- During sustainment, substantial numbers of integrated circuits (ICs) will become obsolete or discontinued increasing supply chain risk
- Aftermarket IC may be introduced as counterfeits
- Adversaries may deliberately target the aftermarket



** A 2012 IDA study looked at Bills of Material for 5 current major defense acquisition programs, characterizing the use of over 3000 unique ICs*

IDA

Key JFAC and T&AM Activities

- Standards and Best Practices Group, charter includes
  - Get important commercial microelectronics industry segments involved in DoD T&AM initiatives
  - Collaborate with related industries (i.e., aerospace, automotive, etc.) and communities to develop alignment with DoD T&AM approaches, practices, and guidance and promote their adoption
  - Engage with industry to leverage existing practices and standards and develop key new standards that support DoD T&AM program objectives
  - Assist government and industry in selecting and leveraging available standards

- FPGA Assurance Group
  - DoD FPGA Assurance Strategy – in development

FPGA Assurance Strategy Overview

- A coherent, focused strategy document for FPGA assurance that will:
  - Enhance FPGA Assurance: Leverage research and capabilities across the DoD, industry, and academia.
  - Focus and Align Resources: Leverage collaboration and the identification, alignment, and application of investments in research and in capabilities across the U.S. Government (USG), industry, and academia to support the larger DoD and USG microelectronics strategies.
  - Policy, Guidance, and Standards: Update and clarify assurance-related policy and guidance to reflect consistent use of current and emerging assurance technology, standardize assurance community knowledge, and provide a platform for outreach to communicate related policies, guidance, and standards to the community.
  - Supply Chain Assurance: Focus on the changes in business/procurement practices that are needed to enable this and the broader DoD microelectronics strategy, as well as those needed for DoD to become a better customer, facilitate economies of scale, and mitigate supply chain risk.

Summary

- Microelectronics obsolescence is a DoD assurance concern, e.g., adversaries may taint the aftermarket
- The supply chain for microelectronics is global
  - Not everyone in the supply chain is necessarily friendly
- Key HwA standards areas:
  - Counterfeit prevention and detection
  - Verification and validation
  - Industry standards that increase assurance, e.g., chain of custody
  - Other, e.g., new assurance methods
- Industry standards are important to DoD's HwA efforts
  - Enables programs to be more efficient by focusing the program on establishing HwA requirements and suppliers on solutions