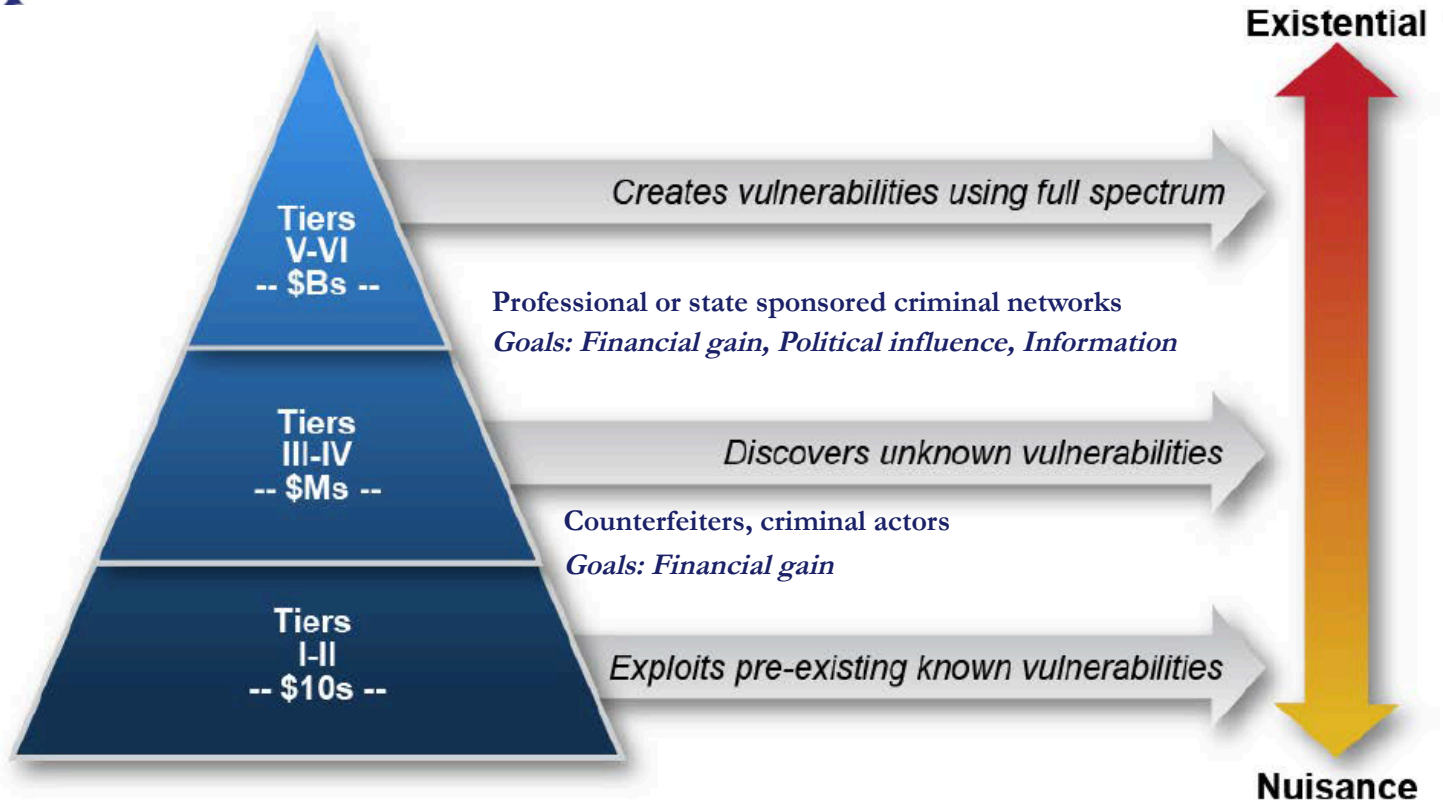
POTOMAC INSTITUTE FOR POLICY STUDIES

Tiers of Trust

A National Strategy for US Government Access to Trusted and Assured Microelectronics As specified in FY17 NDAA Sec. 231

August 16, 2017

DSB Defined Tiers of Threat



Hardware Cyber Threat Spectrum

Anyone can hack software. It takes a nation state to attack hardware.

Hardware attacks are by Nation state actors, capable of insertions across the supply chain; significant resources and expertise required.

Goals: Strategic political, economic, military dominance

Hardware Vulnerabilities created/inserted across supply chain

Existing software and hardware vulnerabilities exploited

Existing software/human vulnerabilities exploited

Creates vulnerabilities using full spectrum

Professional or state sponsored criminal networks

Goals: Financial gain, Political influence, Information

Discovers unknown vulnerabilities

Counterfeiters, criminal actors

Goals: Financial gain

Exploits pre-existing known vulnerabilities

Existential

Nuisance

DSB Task Force Report: Resilient Military Systems and the Advanced Cyber Threat.
http://www.acq.osd.mil/dsb/reports/2010s/ResilientMilitarySystemsCyberThreat.pdf

Threats to the Hardware Supply Chain

Hardware threats exist throughout the global microelectronics supply chain

The Supply Chain – From design and production to deployment
Malicious insertions, Counterfeits, Clones, Insider Threat

Research & Design
(Research, Development, Prototyping)

- Un-vetted 3rd party IP increases the number of people with knowledge of a design and provides opportunities to corrupt a design
- Zero Day effects can be embedded into a chip's design, go undetected, and be triggered after a chip has been produced

Tier IV, V, VI

Production
(Fabrication)

- The U.S. is increasingly relying on off-shore foundries to supply components for our critical mission systems
- Only 2% of ASICs used in National Security Space systems come from DoD trusted foundries
- This increases the risk of malicious insertion to include Trojan horses, Kill Switches, and Backdoors

Tier V, VI

https://www.bloomberg.com/news/articles/2008-10-01/dangerous-fakes

Supply, Stock and Store
(Testing and Verification, Acquisition)

- Attack vectors exist throughout the entire supply chain to include – design, fabrication, testing, packaging, distribution, and end-of-life
- 53% of counterfeit incidents from 2003 – 2013 were for discontinued (legacy) components

Tier I, II, III

Deployment
(Deployed mission systems, Logistics & Maintenance, end-of-life)

- Insider threats and counterfeits in the upgrade/refresh process
- Information exploitation
- Electronic warfare
- Kill switches and backdoors can be used
- Poor disposal practices

Tier IV, V

https://www.slideshare.net/rorykingihs?utm_campaign=profiletracking&utm_medium=sssite&utm_source=ssslideview

http://www.aerospace.org/news/highlights/new-cybersecurity-section-protects-against-hardware-borne-threats/

FY17 NDAA SEC 231. Strategy for Assured Access to Trusted Microelectronics

The Secretary of Defense is shall develop a strategy to ensure that the DoD has assured access to trusted microelectronics, to include:

1) **Definitions of the various levels of trust required by classes of DoD systems**
2) **Means of classifying systems of the DoD based on the level of trust such systems are required to maintain with respect to microelectronics**
3) **Means by which trust in microelectronics can be assured**
4) **Means to increase the supplier base for assured microelectronics to ensure multiple supply pathways**
5) **An assessment of the microelectronics needs of the DoD in future years, including the need for trusted, rad-hard microelectronics**
6) **An assessment of the microelectronics needs of the DoD that may not be fulfilled by entities outside the DoD**
7) **The resources required to assure access to trusted microelectronics, including infrastructure, workforce, and investments in science and technology**
8) **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 need for trust**
9) **Recommendations for changes in authorities, regulations, and practices, including acquisition policies, financial management, public-private partnerships policies, or in any other relevant areas, that would support the achievement of the goals of the strategy**

Presidential Executive Order on Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States (July 21, 2017)

I. Policy: A healthy manufacturing and defense industrial base and resilient supply chains are essential to the economic strength and national security of the United States.

II. Assessment of the Manufacturing Capacity, Defense Industrial Base, and Supply Chain Resiliency of the United States.

1) Report due within 270 days (April 17, 2018)

2) Lead: Sec Defense. Coordinate with: Sec Commerce, Labor, Energy, Homeland Security. Consult with Sec Interior, HHS, OMB, DNI, Asst to President for National Security Affairs, Asst to President on Economic Policy, Office of Trade and Manufacturing Policy, others as needed.

3) Assessment to include:

a) Identify materiel/goods essential to national security

b) Identify manufacturing capabilities essential to (a) above, including emerging capabilities

c) Identify disruptions/compromise/risks to supply chain that are likely

d) Assess resiliency and capacity of manufacturing and defense industrial base and supply chains to meet national security needs:

i. Manufacturing and physical capacity of the DIB, and ability to modernize

ii. Gaps in DIB including non-existent, extinct, threatened and single-point-of-failure capabilities

iii. Supply chains with single point of failure or limited resiliency, including 3rd tier and lower suppliers

iv. Energy consumption and opportunities to increase resiliency through better energy management

v. Domestic education and manufacturing workforce skills

vi. Supply chain risks of potentially unfriendly/unstable nations

vii. Availability of substitute or alternative sources

e) Identify the causes of DIB/supply chain gaps assessed in (d)

f) Recommend legislative, regulatory, policy changes, and assess benefits/costs (economic, strategic, national security) over short, medium, and long terms, to avoid/prepare for/ameliorate gaps and strengthen DIB and increase supply chain resiliency.

Rationalizing & Integrating DoD Capabilities

The Trusted Microelectronics Supply Chain

Research & Design → **Production** → **Supply, Stock & Store** → **Deployment**

- Research for trusted design & manufacturing
- Manage relationship with Industry for R&D access to "pre-SOTA" technology
- Focus on research, design, and prototyping
- Acquisition of IP for pre-fab research

SOTA → Trusted Foundry (GF)

SOTP → Trusted Commercial Suppliers (79 Suppliers)

Legacy → DMEA (Flexible Foundry)

ASD(R&E)

JFAC Steering Committee

- SwA Technical Working Group
- HwA Technical Working Group

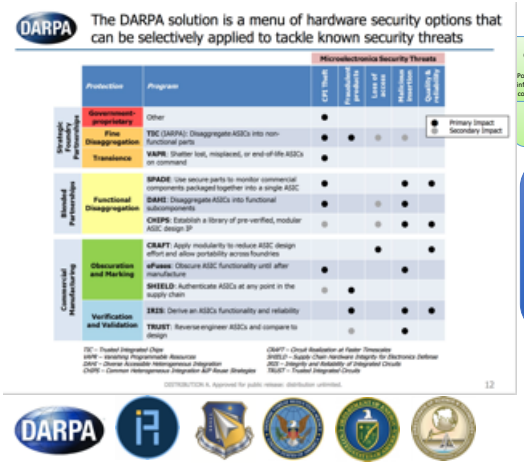
Armed Services need new policies to secure deployed systems

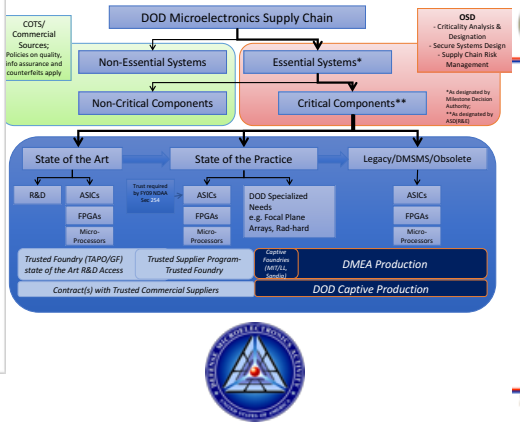
Strategy: Address the entire supply chain

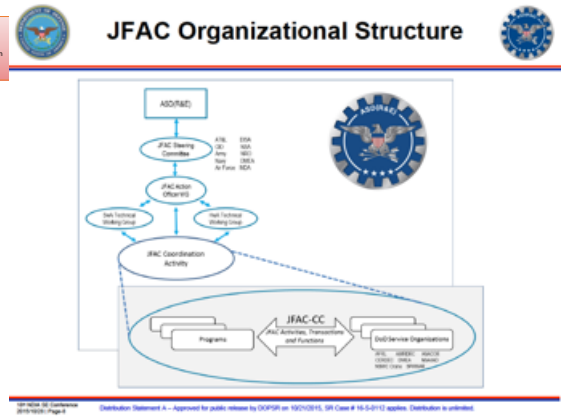
US Government Solution – DMEA Executive Agent

The Trusted Microelectronics Supply Chain

Research & Design → **Production** → **Supply, Stock & Store** → **Deployment**







Designate DMEA as Executive Agent

Current DoD Policies Include:

- Defense Industrial Base Sector Specific Plan (2010)
- Mission Assurance Strategy (2012)
- Antiterrorism Force Protection
- Counterfeit Mitigation Policies

FY17 NDAA Sec 231 Mapped to DOD Responsible Organization

The Trusted Microelectronics Supply Chain

Research & Design → **Production** → **Supply, Stock & Store** → **Deployment**

DARPA

(7) Resources: Invest in future infrastructure, workforce, and science and technology needed to assure access to Trusted Microelectronics, both from commercial sources and within DoD *[See (4), (5), (6), (8)]*
(8) R&D Strategy for State of the Art Access: DoD is pursuing a research and development strategy to, where practicable, use state of the art commercial microelectronics capabilities or their equivalent, while satisfying the need for trust, and to partner with industry to drive future developments in electronics. (Co-leads: DARPA and AFRL.) This includes investments in DARPA MTO's research portfolio and Electronics Resurgence Initiative
(9) c) DARPA should be designated the lead for Trust research & development (R&D) efforts across the DOD, DOE, and Intelligence Community.

DMEA –Executive Agent

(1) and (2) Establish Policy and Definitions of Levels of Trust: DoD is developing policy on the various levels of trust required by classes of DoD systems.
(3) Assure trust in microelectronics via three complementary means: a) Use commercial sources whenever possible, b) Develop and utilize technologies and techniques for assuring Trust, c) Ensure a long term backup plan (DMEA Flexible Foundry).
(4) Increase the commercial supplier base to ensure multiple supply pathways. Continue and expand accreditation through the DMEA Trusted Supplier Program and defense industrial base infrastructure investments when needed.
(5) Assess and plan for future anticipated microelectronics needs. DoD anticipates a broad spectrum of future trusted microelectronics needs from commercial to highly secure, including specialty technologies and defense-specific capabilities such as rad-hard. Invest in the Armed Services to refresh critical vulnerable components and develop supply chain risk management and threat mitigation policy and tools.
(6) Ensure a long-term backup plan to assure access for future microelectronics needs that may not be fulfilled by entities outside DoD. In order to assure a future supply of critical microelectronics DoD will need to invest in maintaining backup design and production capabilities within DoD. This includes investments in 300mm advanced node and split fabrication production capabilities at DMEA's Flexible Foundry.
(9) b) DMEA should be elevated to an agency and should be designated the executive agent for providing assured access to trusted microelectronics for the entire US Government.

JFAC

(9) d) The Joint Federated Assurance Center (JFAC) should coordinate hardware verification and validation (V&V) for the entire USG.

SERVICES

(9) e) The Armed Services should develop policy and regulations for supply chain risk management and threat mitigation during acquisition, sustainment, and end of life.

Policy Recommendations

FY17 NDAA Sec 231 (9)

DMEA should be elevated to an agency and should be designated the executive agent for providing assured access to trusted microelectronics for the entire US Government.

- **Research & Design:**
  - **(7) Resources: Invest in future infrastructure, workforce, and science and technology** needed to assure access to Trusted Microelectronics, both from commercial sources and within DoD *[See (4), (5), (6), (8)]*
  - **(8) R&D Strategy for State of the Art Access:** DoD is pursuing a research and development strategy to, where practicable, use state of the art commercial microelectronics capabilities or their equivalent, while satisfying the need for trust, and to partner with industry to drive future developments in electronics. (Co-leads: DARPA and AFRL.) This includes investments in DARPA MTO's research portfolio and Electronics Resurgence Initiative.
  - **(9) c)** DARPA should be designated the lead for Trust research & development (R&D) efforts across the DOD, DOE, and Intelligence Community.
- **Production:**
  - **(1) and (2) Establish Policy and Definitions of Levels of Trust: DoD is developing policy on the various levels of trust** required by classes of DoD systems. DoD is developing a means of classifying systems based on the level of trust such systems are required to maintain with respect to microelectronics, to expand upon the current trust definition (DODI 5200.44).
  - **3) Assure trust in microelectronics** via three complementary means: a) Use commercial sources whenever possible, b) Develop and utilize technologies and techniques for assuring Trust, and c) Ensure a long-term backup plan (government owned and operated capability at DMEA).
  - **(4) Increase the commercial supplier base to ensure multiple supply pathways.** Continue and expand accreditation through the DMEA Trusted Supplier Program and defense industrial base infrastructure investments when needed.
  - **(5)** Assess and plan for future anticipated microelectronics needs. DoD anticipates a broad spectrum of future trusted microelectronics needs from commercial to highly secure, including specialty technologies and defense-specific capabilities such as rad-hard. Invest in the Armed Services to refresh critical vulnerable components and develop supply chain risk management and threat mitigation policy and tools**(3**
  - **(6) Ensure a long-term backup plan to assure access for future microelectronics needs that may not be fulfilled by entities outside DoD.** In order to assure a future supply of critical microelectronics DoD will need to invest in maintaining backup design and production capabilities within DoD. This includes investments in 300mm advanced node and split fabrication production capabilities at DMEA's Flexible Foundry
  - **(9) b)** DMEA should be elevated to an agency and should be designated the executive agent for providing assured access to trusted microelectronics for the entire US Government.
- **Supply, Stock and Store:**
  - **(9) d)** The Joint Federated Assurance Center (JFAC) should coordinate hardware verification and validation (V&V) for the entire USG.
- **Deployment:**
  - **(9) e)** The Armed Services should develop policy and regulations for supply chain risk management and threat mitigation during acquisition, sustainment, and end of life.
- (9) a) DoD should be designated the lead agency across the US Government on Assured Access to Trusted Microelectronics, and coordinate with Department of Energy and ODNI to establish joint

Questions?