# Department of Defense (DoD) Trusted Microelectronics

**Raymond Shanahan**

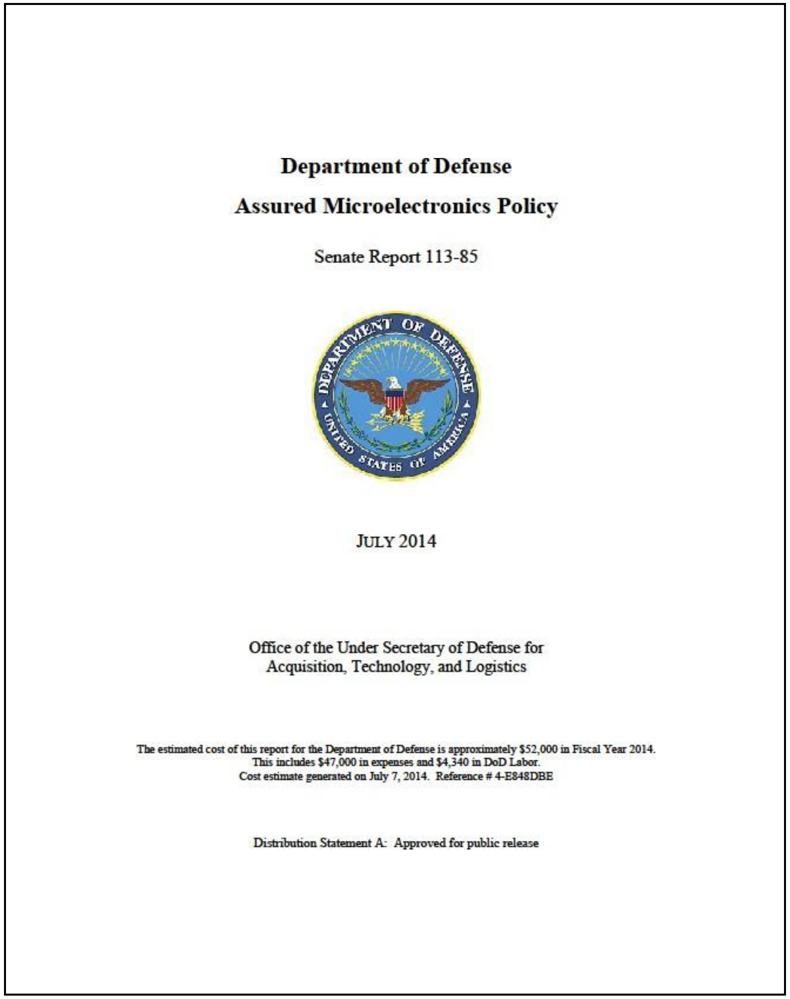
**Office of the Deputy Assistant Secretary of Defense for Systems Engineering (DASD(SE))**

**17th Annual NDIA Systems Engineering Conference**
**Springfield, VA | October 29, 2014**

Distribution Statement A – Approved for public release by DOPSR. Distribution is unlimited.

# Outline

- **Beyond Application-Specific Integrated Circuits (ASICs)**
- **Identifying critical functions and components**
- **Analyzing risk and identifying mitigations**
- **Leveraging existing policies and guidance**



**Department of Defense**

**Assured Microelectronics Policy**

Senate Report 113-85

JULY 2014

Office of the Under Secretary of Defense for
Acquisition, Technology, and Logistics

The estimated cost of this report for the Department of Defense is approximately $52,000 in Fiscal Year 2014.
This includes $47,000 in expenses and $4,340 in DoD Labor.
Cost estimate generated on July 7, 2014.  Reference # 4-E848DBE

Distribution Statement A:  Approved for public release

http://www.acq.osd.mil/se/docs/DoD-Assured-Microelectronics-Policy-RTC-July2014.pdf

# Problem Statement

## Vulnerabilities in supply chain could lead to malicious logic insertions

- **Current DoD-unique ASICs used in DoD systems are procured via a Trusted Supplier chain per DoD policy**
  - Accounts for approximately 10% of logic-bearing DoD Integrated Circuit (IC) products used in DoD systems
- **Approximately 72% of DoD ICs are non-ASICs; largely Field Programmable Gate Array (FPGA) devices**
  - DoD has no current trusted supply chain for FPGAs
  - FPGAs include COTS and Military grade products
  - Much of the FPGA value chain is off-shore, e.g., design, fabrication, programming services, testing and packaging
- **FPGAs that are programmed by DoD end-users may face Software Assurance (SwA) risks in FPGA bitstream programming tools, environment, and processes**
- **Bottom line: ASICs and FPGAs are not the only ICs of concern (must address more than ASIC foundry operations)**

Distribution Statement A – Approved for public release by DOPSR. Distribution is unlimited.

# Real World Example

## Bill of Material (BOM) excerpt from Program Protection Plan (PPP) review

| LV | Part Number | Nomenclature | QPA | Unit Price | Material |
|---|---|---|---|---|---|
| 03 | 602358-029 | ABC SUB/ASSY | 1 | $0.00 | 0.0001 |
| 03 | 0089-1A33 | HUMISEAL,TY UR,CL B,GAL | 0.01 | $0.00 | 0 |
| 03 | MC-0402-875 | POLYURETHAN ADH,875 GM KT | 0.01 | $0.00 | 0 |
| 03 | 25ACL71-M | MAG., MODULE, P/S | 1 | $0.00 | 0.0001 |
| 03 | 030C-M | DC-DC | 1 | $0.00 | 0.0001 |
| 03 | C075F1 | MAG., MODULE, P/S | 1 | $0.00 | 0.0001 |
| 03 | S3755/1-10 | POWDER,FUME SILI 10LB BAG | 0.0001 | $0.00 | 0 |
| 04 | 548FKTWREP | MICROCIRCUIT (REELED) | 12 | $15.01 | 180.1572 |
| 04 | 413ES | MICROCIRCUIT (REELED) | 11 | $9.69 | 106.5559 |
| 05 | 003A0A94 | PWR SUPPLY DC-DC | 1 | $0.00 | 0.0001 |
| 05 | 015C91 | P/S MODULE,DC-DC | 2 | $0.00 | 0.0002 |
| 05 | XYZ-1553GT | MICROCIRCUIT (REELED) | 1 | $428.91 | 428.9061 |
| 05 | 2V500-4FG456I | MCKT (MATRIX TRAYED) | 1 | $199.52 | 199.5246 |
| 05 | 602458-001 | ABC PWB | 1 | $233.12 | 233.1221 |

| | |
|---|---|
| Part number | **XYZ-1553GT** |
| Category | **Communication => Others** |
| Description | Description = **MIL-STD-1553, Dual Redundant, Remote Terminal, 4k Words Static RAM, Multichip, Monolithic Transceivers**<br>**REDACTED VERSION** |

# Real World Example

## Bill of Material (BOM) excerpt from Program Protection Plan (PPP) review

| LV | Part Number | Nomenclature | QPA | Unit Price | Material |
|---|---|---|---|---|---|
| 03 | 602358-029 | ABC SUB/ASSY | 1 | $0.00 | 0.0001 |
| 03 | 0089-1A33 | HUMISEAL,TY UR,CL B,GAL | 0.01 | $0.00 | 0 |
| 03 | MC-0402-875 | POLYURETHAN ADH,875 GM KT | 0.01 | $0.00 | 0 |
| 03 | 25ACL71-M | MAG., MODULE, P/S | 1 | $0.00 | 0.0001 |
| 03 | 030C-M | DC-DC | 1 | $0.00 | 0.0001 |
| 03 | C075F1 | MAG., MODULE, P/S | 1 | $0.00 | 0.0001 |
| 03 | S3755/1-10 | POWDER,FUME SILI 10LB BAG | 0.0001 | $0.00 | 0 |
| 04 | 548FKTWREP | MICROCIRCUIT (REELED) | 12 | $15.01 | 180.1572 |
| 04 | 413ES | MICROCIRCUIT (REELED) | 11 | $9.69 | 106.5559 |
| 05 | 003A0A94 | PWR SUPPLY DC-DC | 1 | $0.00 | 0.0001 |
| 05 | 015C91 | P/S MODULE,DC-DC | 2 | $0.00 | 0.0002 |
| 05 | XYZ-1553GT | MICROCIRCUIT (REELED) | 1 | $428.91 | 428.9061 |
| 05 | 2V500-4FG456I | MCKT (MATRIX TRAYED) | 1 | $199.52 | 199.5246 |
| 05 | 602458-001 | ABC PWB | 1 | $233.12 | 233.1221 |

| | |
|---|---|
| Part number | XYZ-1553GT |
| Category | Communication => Others |
| Description | Description = MIL-STD-1553 Dual Redundant, Remote Terminal, 4k Words Static RAM, Multichip Monolithic Transceivers |

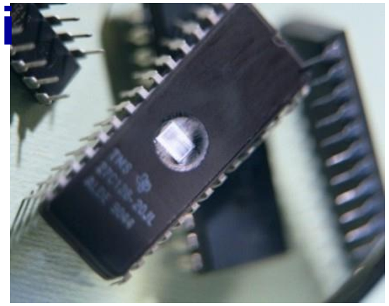
REDACTED VERSION

A MIL-STD data bus interface designed for use with military avionics, but also commonly used in spacecraft; functions as a programmable remote terminal consisting of a protocol chip, 2 transceivers & 16K SRAM

Made in U.S., but sold world-wide

# Microelectronics Assurance Policy Objective

- **Implement Supply Chain Risk Management (SCRM) on microelectronics components used in National Security Systems when military end use is identifiable, thus targetable for malicious acts; in particular, when:**
  - Used in intelligence, crypto, command & control, and weapon systems,
  - Critical to military or intelligence mission success, or
  - They manage classified information
- **Microelectronic component attributes of interest, i**
  - Define a sequence of instructions,
  - Perform one or more decision making functions,
  - Execute basic units of logic,
  - Can be altered surreptitiously to trigger malicious functionality or the loss of confidential information.



- **Examples of microelectronics that may be critical include custom ASICs, programmable logic devices (e.g., FPGAs), micro-processors, Application Specific Standard Products, and flash memories**

**How do we find them and mitigate the risk?**

Distribution Statement A – Approved for public release by DOPSR. Distribution is unlimited.

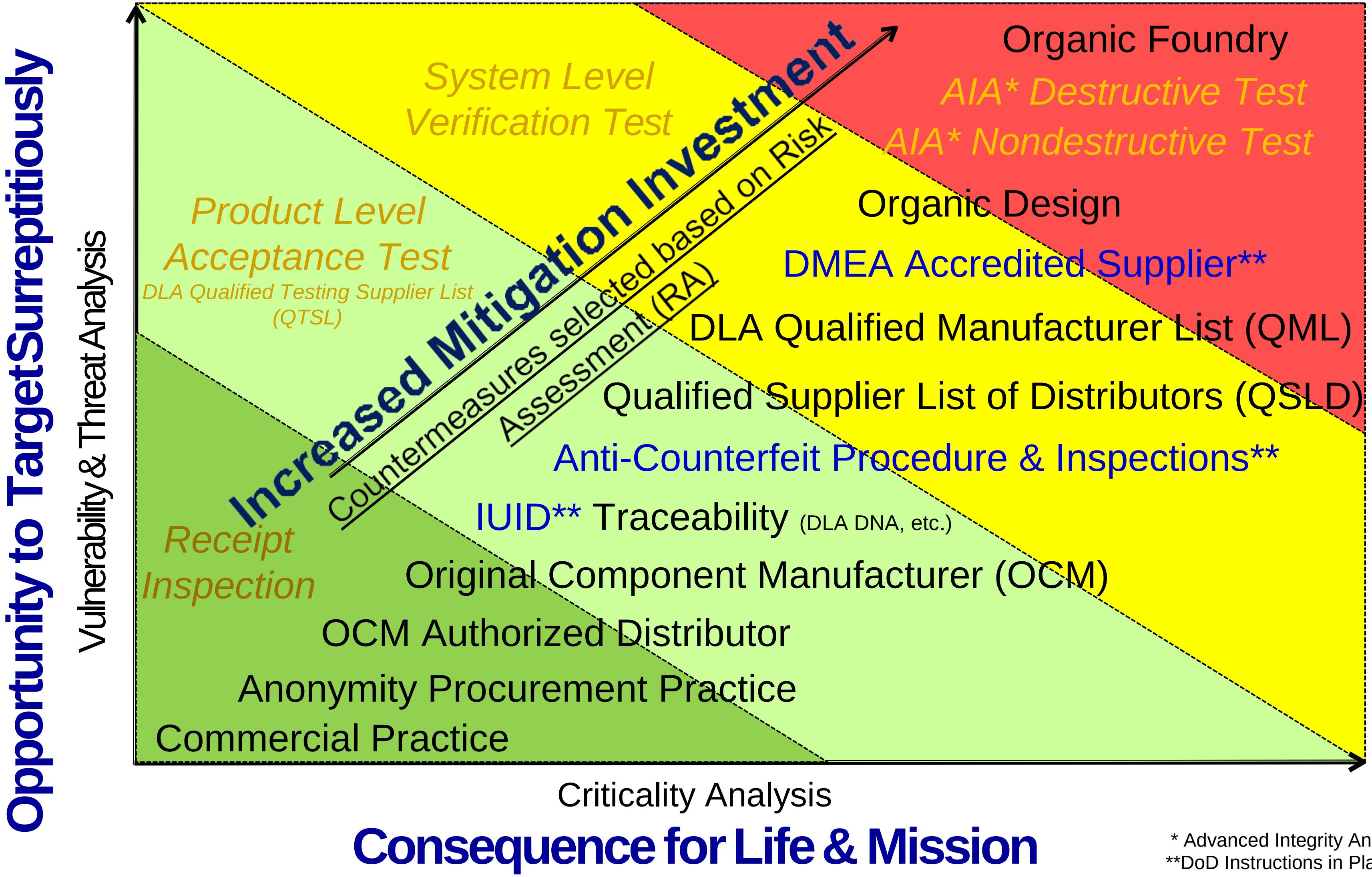
# What is Critical?

- **To execute policy and guidance beyond identifying ASICs, programs need to identify mission critical functions and components**

  - Programs lack visibility into most of the microelectronics used in systems
  - Prior to Critical Design Review (CDR), the system configuration and sources of supply are still subject to change
  - During program development, programs should require contractors and their suppliers to identify and nominate Level I and II critical components (CCs) for protection based on the program's criticality analysis of their assessed risk to mission
  - System configuration data is needed prior to CDR and Bill of Material (BOM) information after CDR to support identification of Level I and II CCs to be protected in accordance with DoDI 5200.44 and DAG Chapter 13

Distribution Statement A – Approved for public release by DOPSR. Distribution is unlimited.

# Supply Chain Risk Countermeasures



Organic Foundry

*AIA* Destructive Test*

*AIA* Nondestructive Test*

*System Level Verification Test*

Organic Design

DMEA Accredited Supplier**

DLA Qualified Manufacturer List (QML)

*Product Level Acceptance Test*

*DLA Qualified Testing Supplier List (QTSL)*

Qualified Supplier List of Distributors (QSLD)

Anti-Counterfeit Procedure & Inspections**

IUID** Traceability (DLA DNA, etc.)

*Receipt Inspection*

Original Component Manufacturer (OCM)

OCM Authorized Distributor

Anonymity Procurement Practice

Commercial Practice

**Increased Mitigation Investment**

Countermeasures selected based on Risk Assessment (RA)

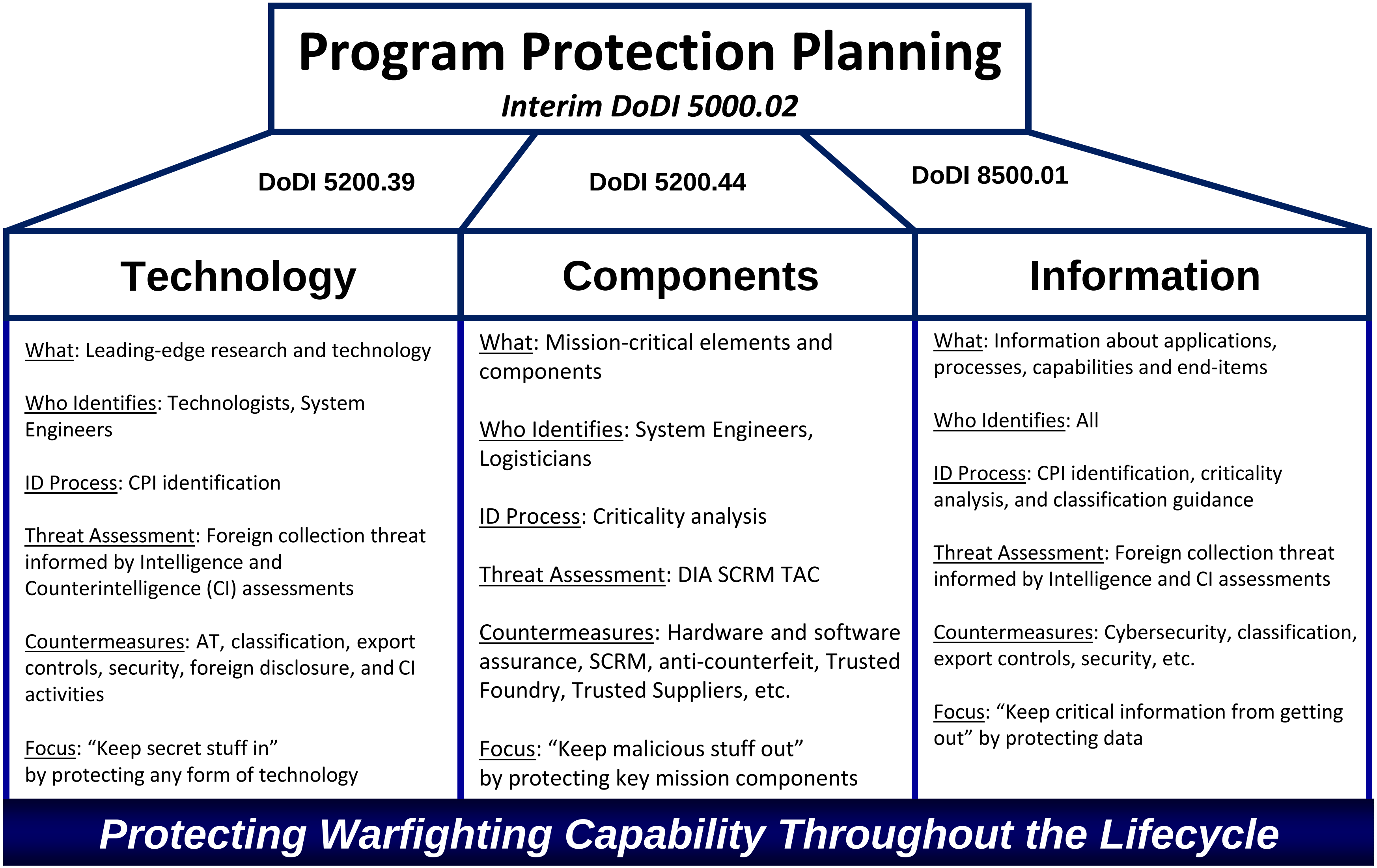
Opportunity to Target Surreptitiously
Vulnerability & Threat Analysis
Criticality Analysis
Consequence for Life & Mission

* Advanced Integrity Analysis (AIA)

**DoD Instructions in Place

Distribution Statement A – Approved for public release by DOPSR. Distribution is unlimited.

# What Are We Protecting?



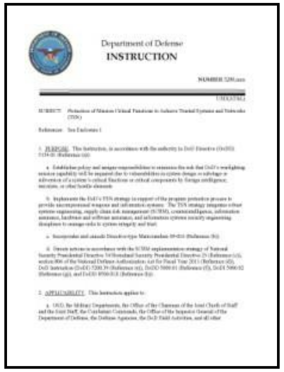
## Program Protection Planning

*Interim DoDI 5000.02*

| DoDI 5200.39 | DoDI 5200.44 | DoDI 8500.01 |
|---|---|---|
| **Technology** | **Components** | **Information** |
| What: Leading-edge research and technology | What: Mission-critical elements and components | What: Information about applications, processes, capabilities and end-items |
| Who Identifies: Technologists, System Engineers | Who Identifies: System Engineers, Logisticians | Who Identifies: All |
| ID Process: CPI identification | ID Process: Criticality analysis | ID Process: CPI identification, criticality analysis, and classification guidance |
| Threat Assessment: Foreign collection threat informed by Intelligence and Counterintelligence (CI) assessments | Threat Assessment: DIA SCRM TAC | Threat Assessment: Foreign collection threat informed by Intelligence and CI assessments |
| Countermeasures: AT, classification, export controls, security, foreign disclosure, and CI activities | Countermeasures: Hardware and software assurance, SCRM, anti-counterfeit, Trusted Foundry, Trusted Suppliers, etc. | Countermeasures: Cybersecurity, classification, export controls, security, etc. |
| Focus: "Keep secret stuff in"<br>by protecting any form of technology | Focus: "Keep malicious stuff out"<br>by protecting key mission components | Focus: "Keep critical information from getting out" by protecting data |

***Protecting Warfighting Capability Throughout the Lifecycle***

# Program Protection
# Integrated Supply Chain Policy



Department of Defense
INSTRUCTION

NUMBER 5200.44

SUBJECT: Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)

References: See Enclosure 1

1. PURPOSE. [illegible]

2. APPLICABILITY. This Instruction applies to: [illegible]

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

- – Requires AT&L to develop a strategy for managing risk in the supply chain for integrated circuit-related products and services (e.g., FPGAs, printed circuit boards) that are identifiable to the supplier as specifically created or modified for DoD (e.g., military temperature range, radiation hardened).

DoD 4140.1-R

DEPARTMENT OF DEFENSE

DoD
Supply Chain Materiel
Management Regulation

MAY 23, 2003

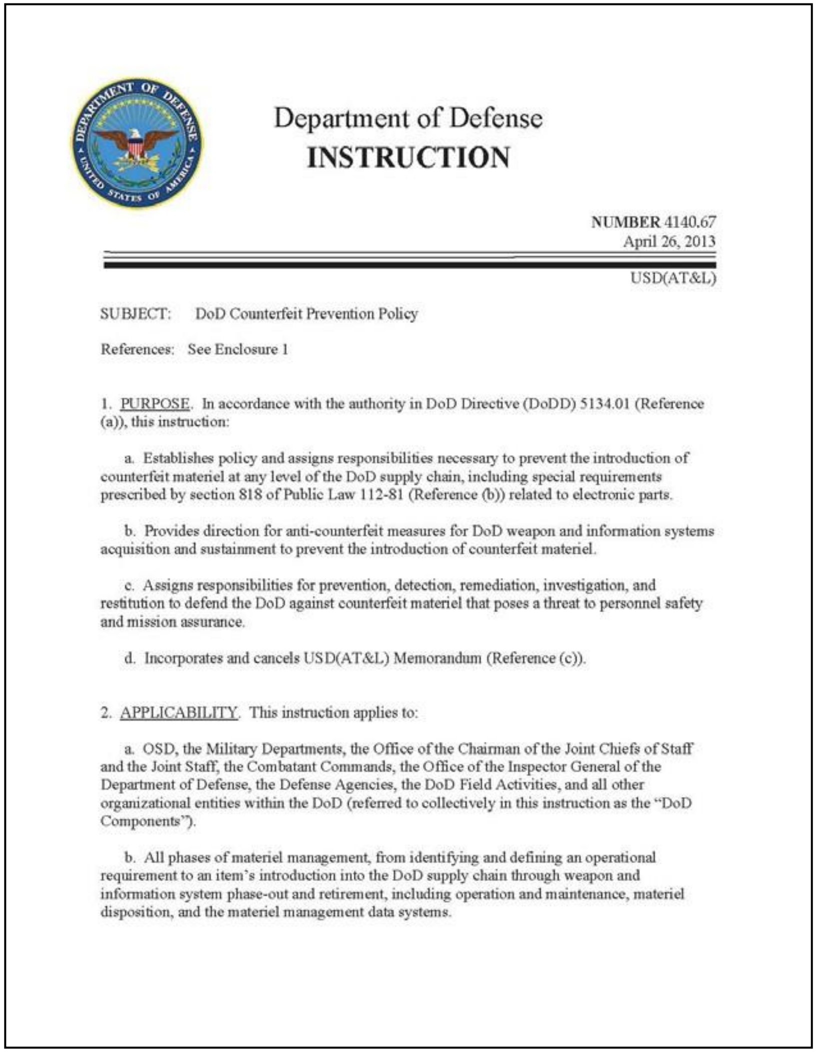
Office of the Deputy Under Secretary of Defense for
Logistics and Materiel Readiness

## DoD 4140.1-R, DoD Supply Chain Materiel Management Regulation

- – Requires quality assurance methods including contractor selection and qualification programs; quality requirements; pre-award surveys; Government inspection; and testing.
- – Quality assurance techniques and testing should <u>stress conforming Critical Application Item (CAI) to contract and technical requirements</u>.

**Security risk criteria should be added to safety, reliability, etc. for CAI designation in the supply chain to assist in managing microelectronics CCs throughout the acquisition lifecycle**

# DoDI 4140.67
# DoD Counterfeit Prevention Policy



Department of Defense
**INSTRUCTION**

NUMBER 4140.67
April 26, 2013

USD(AT&L)

SUBJECT: DoD Counterfeit Prevention Policy

References: See Enclosure 1

1. PURPOSE. In accordance with the authority in DoD Directive (DoDD) 5134.01 (Reference (a)), this instruction:

a. Establishes policy and assigns responsibilities necessary to prevent the introduction of counterfeit materiel at any level of the DoD supply chain, including special requirements prescribed by section 818 of Public Law 112-81 (Reference (b)) related to electronic parts.

b. Provides direction for anti-counterfeit measures for DoD weapon and information systems acquisition and sustainment to prevent the introduction of counterfeit materiel.

c. Assigns responsibilities for prevention, detection, remediation, investigation, and restitution to defend the DoD against counterfeit materiel that poses a threat to personnel safety and mission assurance.

d. Incorporates and cancels USD(AT&L) Memorandum (Reference (c)).

2. APPLICABILITY. This instruction applies to:

a. 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").

b. All phases of materiel management, from identifying and defining an operational requirement to an item's introduction into the DoD supply chain through weapon and information system phase-out and retirement, including operation and maintenance, materiel disposition, and the materiel management data systems.

- **Implements DoD counterfeit prevention strategy**
  - Requires procurement of critical electronic parts from suppliers that meet risk-based criteria
  - Applies additional measures when such suppliers not available

- **Counterfeit defined as:**
  - "Unauthorized copy or substitute that has been identified, marked, or altered by a source other than the item's legally authorized source"
  - "Misrepresented to be an authorized item of the legally authorized source

# ASIC Policy and Guidance

**In applicable systems,* IC-related products and services shall be procured from a trusted supplier accredited by the DMEA when they are custom-designed, custom-manufactured, or tailored for a specific DoD military end use i.e., ASICs – DoDI 5200.44**

- **Program Protection Plan (PPP) identifies custom ASICs incorporated in the system design**
- **PPP describes plan to utilize trusted suppliers for the ASICs**
- **Accredited trusted suppliers can be found at: http://www.dmea.osd.mil/trustedic.html**

***Applicable systems**:
(1) National security systems as defined by section 3542 of title 44, United States Code (U.S.C.) (Reference (l));
(2) Mission Assurance Category (MAC) I systems, as defined by Reference (j); or
(3) Other DoD information systems that the DoD Component's acquisition executive or chief information officer determines are critical to the direct fulfillment of military or intelligence missions."

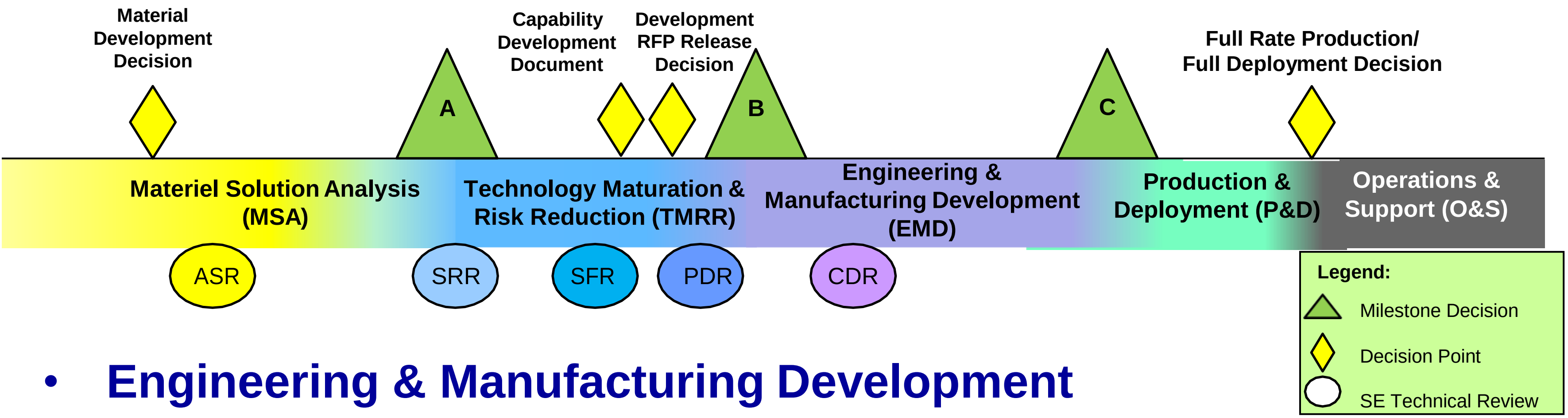
# IC Policy and Guidance

**Control the quality, configuration, and security of software, firmware, hardware, and systems throughout their lifecycles, including components or subcomponents from secondary sources. Employ protections that manage risk in the supply chain for components or subcomponent products and services (e.g., ICs, FPGA, printed circuit boards) when they are identifiable (to the supplier) as having a DoD end-use. – DoDI 5200.44**

- **PPP identifies the system's critical functions and CCs**
  - Custom ASICs, FPGAs, etc. are identified in this process
- **PPP addresses how protections for CCs are implemented at each program milestone phase:**
  - Component testing, including logic, imaging, signal and thermal testing, and system-level testing
  - Process controls, including anti-counterfeit and supply "chain of custody"

# PPP Milestones

- **Technology Development**
  - Document probable CCs and potential countermeasures
  - Plan life-cycle sustainment of proposed technologies



Material Development Decision
A
Capability Development Document
Development RFP Release Decision
B
C
Full Rate Production/ Full Deployment Decision
Materiel Solution Analysis (MSA)
Technology Maturation & Risk Reduction (TMRR)
Engineering & Manufacturing Development (EMD)
Production & Deployment (P&D)
Operations & Support (O&S)
ASR
SRR
SFR
PDR
CDR
Legend:
Milestone Decision
Decision Point
SE Technical Review

- **Engineering & Manufacturing Development**
  - Protect CCs by implementing appropriate techniques
- **Production & Deployment**
  - Control product baseline for Class 1 configuration changes
- **Operations & Support**
  - Manage CCs and configuration throughout the lifecycle

**Configuration → CDR → Parts**

# Example Collaboration Opportunities

- **Joint Federated Centers for Trusted Defense Systems**
  - FY14 National Defense Authorization Act Section 937
  - Developing the Joint Federated Assurance Center (JFAC) Charter, standing up JFAC software and hardware assurance technical working groups, and executing JFAC pilot activities

- **Microelectronics guidance and best practices**
  - Initiating development of risk-based mitigation strategies and approaches by component type in support of programs through JFAC pilot activities
  - Collaborating with Society of Automotive Engineering Committee G12/JC13.2 in their development of industry best practices for SCRM for microelectronics

- **Industry Forums**
  - NDIA Systems Security Engineering Committee and Workshops
  - NDIA Trusted Supplier Steering Group Workshops
  - Annual GOMACTech Industry Day

Distribution Statement A – Approved for public release by DOPSR. Distribution is unlimited.

# For Additional Information

**Raymond Shanahan**

**Deputy Director, Systems Security Engineering**

**Office of the Deputy Assistant Secretary of Defense,**
**Systems Engineering (ODASD(SE))**

**(571) 372-6558 | raymond.c.shanahan.civ@mail.mil**

# Systems Engineering: Critical to Defense Acquisition

***Defense Innovation Marketplace***
***http://www.defenseinnovation.mil***

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