



Microelectronics (MicroE) Strategy

Raymond Shanahan

**Office of the Deputy Assistant Secretary of Defense
for Systems Engineering, OUSD(AT&L)**

**NDIA Trusted Microelectronics Meeting
January 15, 2014**



Outline



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



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 MicroE 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 & FPGAs are not the only MicroE of concern (must address more than ASIC foundry operations)**



Real World Example



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

<u>LV</u>	<u>Part Number</u>	<u>Nomenclature</u>	<u>QPA</u>	<u>Unit Price</u>	<u>Material</u>
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



Real World Example

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

<u>LV</u>	<u>Part Number</u>	<u>Nomenclature</u>	<u>QPA</u>	<u>Unit Price</u>	<u>Material</u>
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	2V500-4FG4561	MCKT (MATRIX TRAYED)	1	\$199.52	199.5246
05	602458	ABC PWB	1	\$233.12	233.1221

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

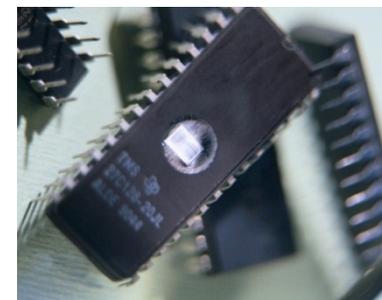
Made in U.S., but sold world-wide



Proposition: Trust Policy Objective



- **Implement Supply Chain Risk Management (SCRM) on MicroE 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
- **MicroE component attributes of interest include, but are not limited to:**
 - Defining a sequence of instructions,
 - Performing one or more decision making functions,
 - Executing basic units of logic,
 - Or, can be altered surreptitiously to trigger malicious functionality or the loss of confidential information.
- **Examples of MicroE that may be critical include vulnerable 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?



Defense Logistics Agency (DLA) Search

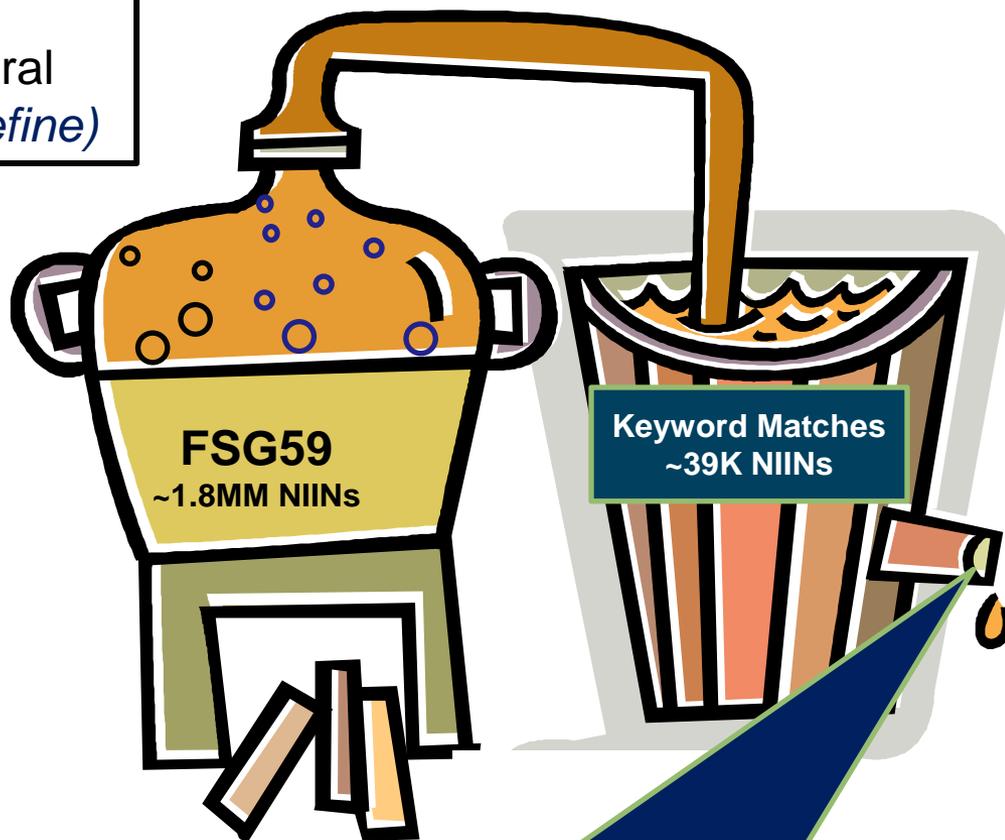
CHALLENGE: How to identify a component as logic-bearing in the federal logistics system? (*working w/DLA to define*)

ASSUMPTIONS:

- Focus is on malicious code risk
- List of 67 “keywords” is sufficient for preliminary data mining efforts
- It is better to include too many National Item Identification Numbers (NIINs) in the final list than not enough
- The Candidate List will continue to morph as more “experts” weigh in

CAVEATS:

- Non-standard data presentation contributes to holes in output
- “Experts” do not agree on all keywords

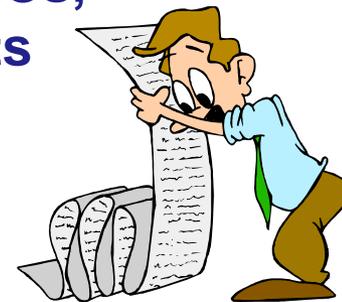


Three categories:
1) Logic-bearing ICT
2) Possibly Logic-bearing ICT
3) Could be Logic-bearing ICT but data insufficient



What is Critical?

- **To execute policy and guidance beyond identifying ASICs, programs need to identify critical functions/components**
 - Programs lack visibility into most of the MicroE used in systems
 - Prior to Critical Design Review (CDR), configuration and sources of supply are uncertain
 - Technology Development Strategy (TDS) will have many gaps
- **Per MIL-HDBK-61A(SE), Configuration Management Guidance: “Designating (*MicroE Critical Components (CCs)*) as Configuration Items increases their visibility and management control throughout the development and support phases.”**
- **To enable DoDI 5200.44 and DAG Chapter 13 compliance for Level I and II CCs, need system configuration data prior to CDR and Bill of Material (BOM) information after CDR**



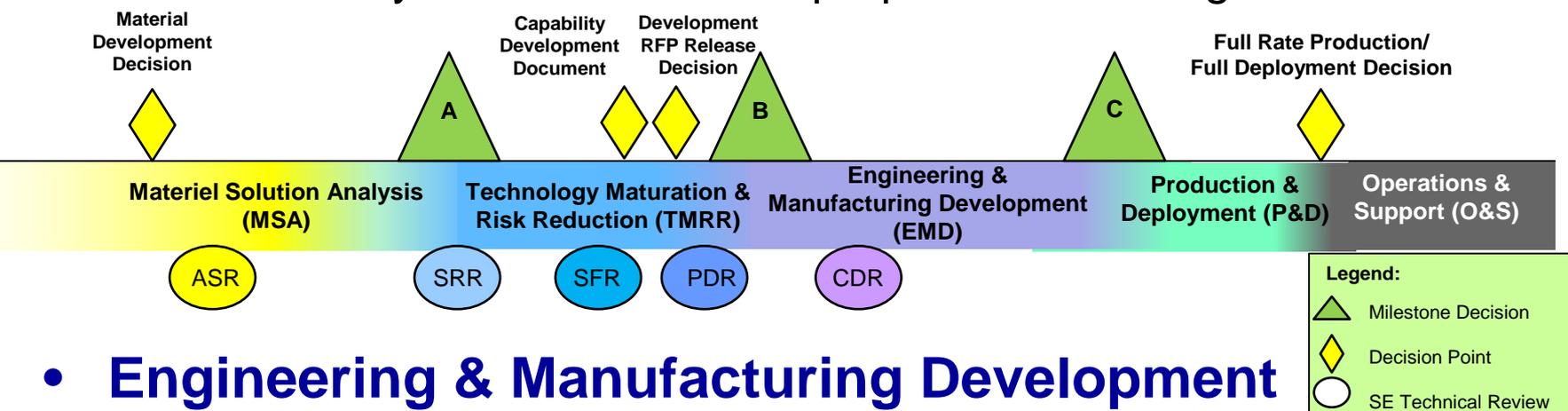
Proposition: During program development, advise contractors and their suppliers of program risk criteria for *MicroE* and require them to identify and nominate CCs based on criticality analysis



PPP Milestones

• Technology Development

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



Configuration → CDR → Parts

• Engineering & Manufacturing Development

- Protect CCs by implementing appropriate techniques

• Production & Deployment

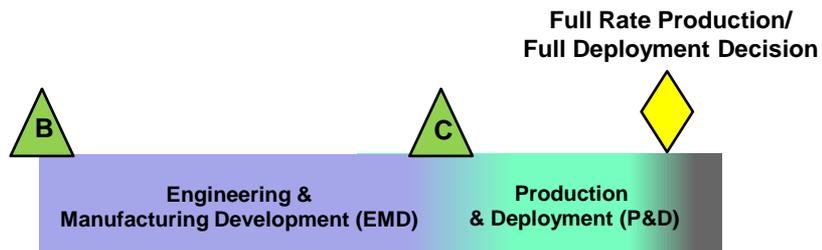
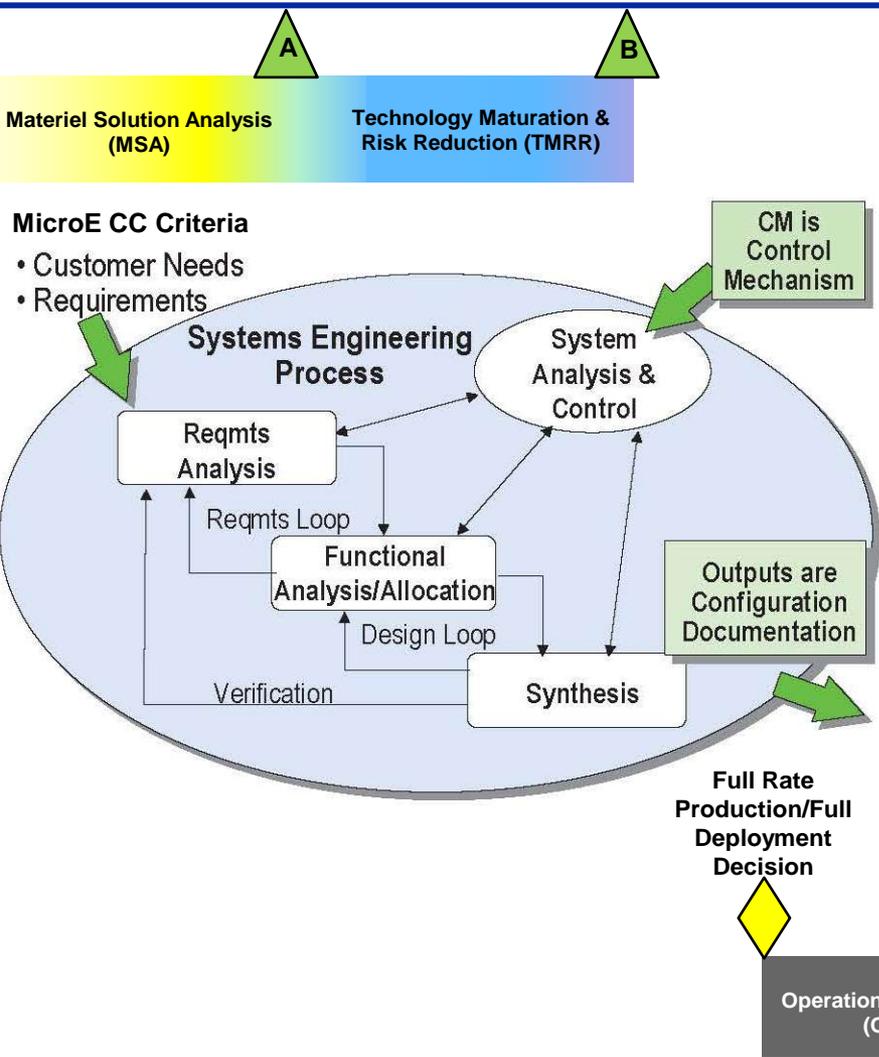
- Control product baseline for Class 1 configuration changes

• Operations & Support

- Manage CCs life-cycle and configuration



Configuration Management (CM) Process



MicroE Controlled Items

- Initially tracked as CC functions
- BOM populated as parts selection made
- Reporting to SE or Engineering Support Activity (ESA) for approval/management
- Special Procedures Code assignment



Life-Cycle Sustainment

- Organic Inventory Reassignment
- Contractor Logistic Support





PPP Data/Info by Milestone



	Matériel Solution Analysis	Technology Maturation & Risk Reduction	Engineering & Manufacturing Development	Production & Deployment/ Operations & Support
Hardware Control (HC):	<p>System-level: Establish initial HC criteria, critical functions and risk mitigation approach.</p>	<p>System-level: Before PDR ensure the identification of all critical functions, known CCs, and product risk mitigations. Component-level: For known Level I/II CCs, consider acceptance inspection/test to mitigate risk of malicious functionality and counterfeit insertion.</p>	<p>System-level: Update HC approach by CDR* identifying all CCs and risk mitigations. Post-CDR, conduct verification test for malicious functionality. Component-level: For Level I/II CCs, consider acceptance test to mitigate risk of malicious code and counterfeit.</p>	<p>System-level: Production and sustainment HC approach to address maintenance for DMSMS concerns during and post-production. Component-level: For Level I/II CCs, consider acceptance test to mitigate risk of malicious functionality and counterfeit.</p>
Supplier/ Supply Chain Control (SC):	<p>System-level: Establish initial SC criteria, critical functions and risk mitigation approach.</p>	<p>System-level: Before PDR to identify process risk mitigations Component-level: 1. Establish component manufacturer qualifications for known CCs, 2. For non-CCs, use commercial & anonymity procurement practice where practicable.</p>	<p>System-level: Updated SC approach before CDR identifying SC risks and mitigations Component-level: 1. ASICs: DMEA Accredited Trusted Services & Flow, 2. Other CCs: Original Component Manufacturer/ Distributor or DLA Qualified Manufacturer/Distributor 3. Anti-counterfeit procedure and Inspections 4. All non-CCs, use anonymity procurement practice where practicable.</p>	<p>System-level: Production and sustainment SC approach before FRP to include maintenance for DMSMS concerns during and post production Component-level: 1. ASICs: DMEA Accredited Trusted Services & Flow 2. Other CCs: Original Component Manufacturer/ Distributor or DLA Qualified Manufacturer/Distributor with chain of custody for CCs 3. Anti-counterfeit procedure and inspections 4. All non-CCs, use anonymity procurement practice where practicable.</p>

**Product:
Critical
Functions /
Components**

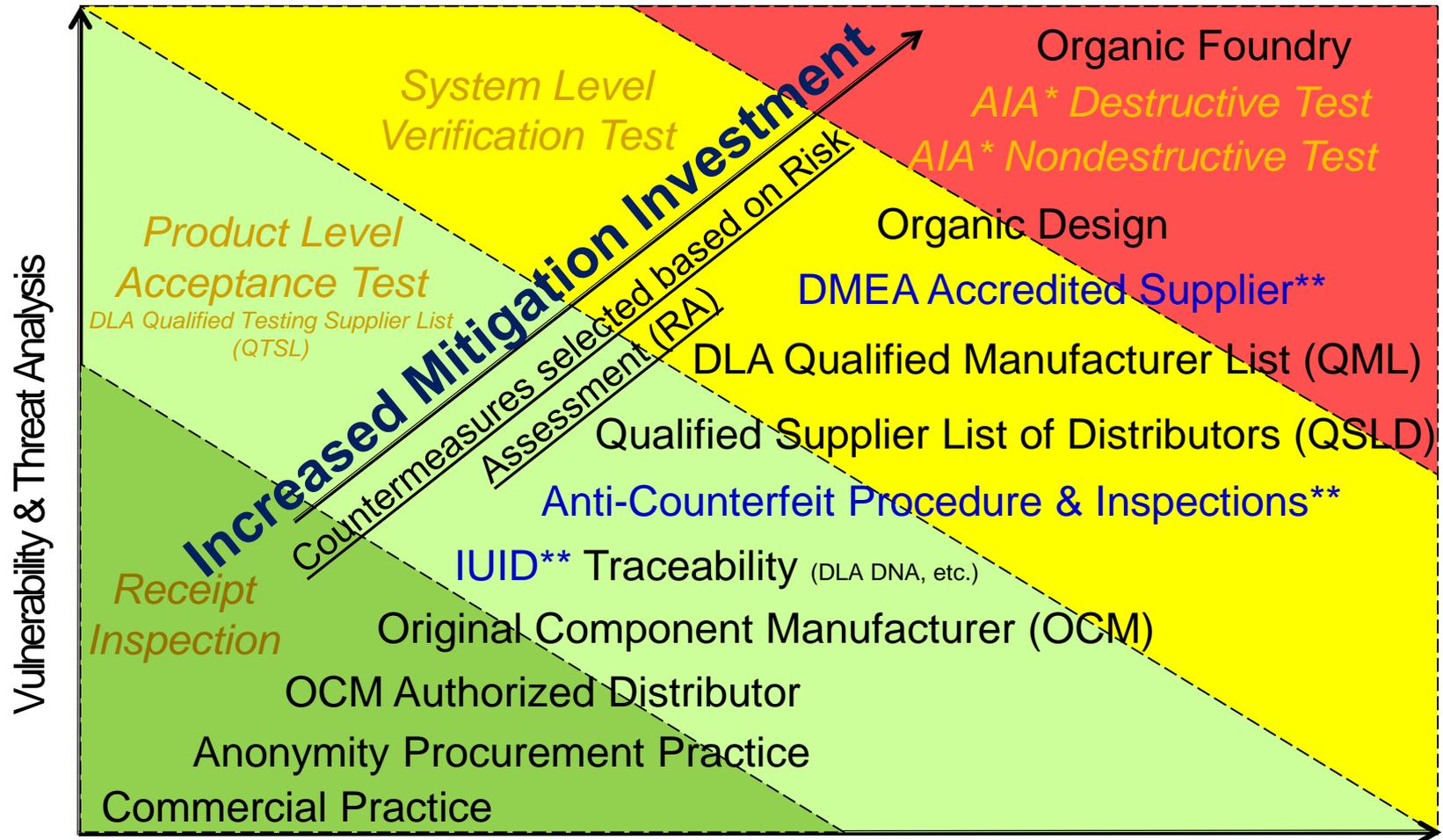
**Process:
-Systems
Integrators,
-Subsystem
Manufacturers
- Critical
Component
Suppliers or
Distributors**

* CC= Critical Component, PDR = Preliminary Design Review, CDR = Critical Design Review, FRP = Full-Rate Production, DMSMS = Diminishing Manufacturing Sources and Material Shortages



Supply Chain Risk Countermeasures

Opportunity to Target Surreptitiously



Consequence for Life & Mission

* Advanced Integrity Analysis (AIA)
 **DoD Instructions in Place



Transition from Configuration to Parts Management

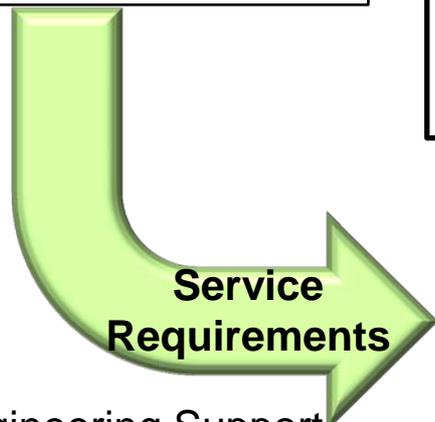
Acquisition Process



Logistics Reassignment Process

- Governed by DoD 4140.26M (Vol 2 & 4)
- Service defines criticality of part or item
 - Critical Flight Safety
 - Critical Application
- Service defines Acquisition Strategy:
 - Sole source
 - Competitive bid

Sustainment Process



Service Engineering Support Activity (ESA) retains configuration control (Tech data)

Wholesale management of consumable items



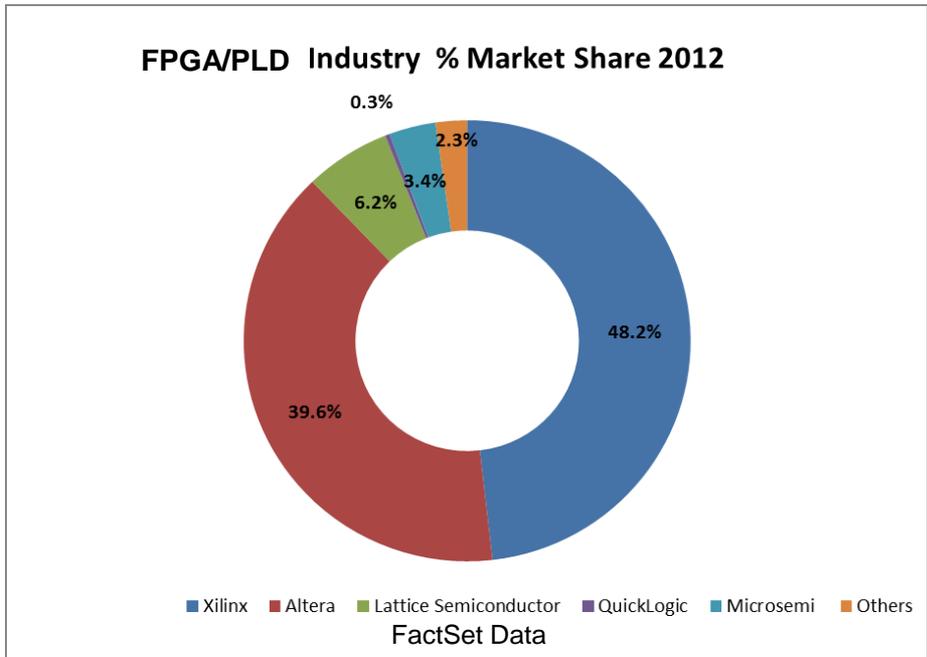
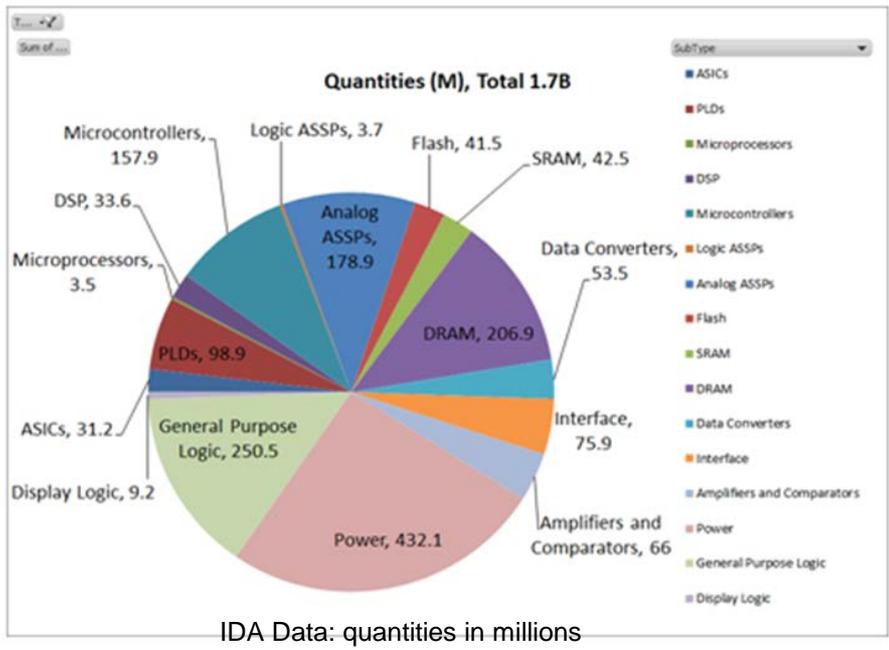
DoD 4140.26M DoD Integrated Materiel Management (IMM) for Consumable Items



Identifying MicroE of Interest

Proposition: Focus trust policy on select devices

- Custom ASIC (57 vendors DMEA accredited)
- Hybrid (54 vendors QML approved by DLA for space apps)
- Semi-custom/tailored FPGA (2 vendors have 88% of DoD market)
- ...Other MicroE meeting criteria (*developing mitigations w/DMEA*)



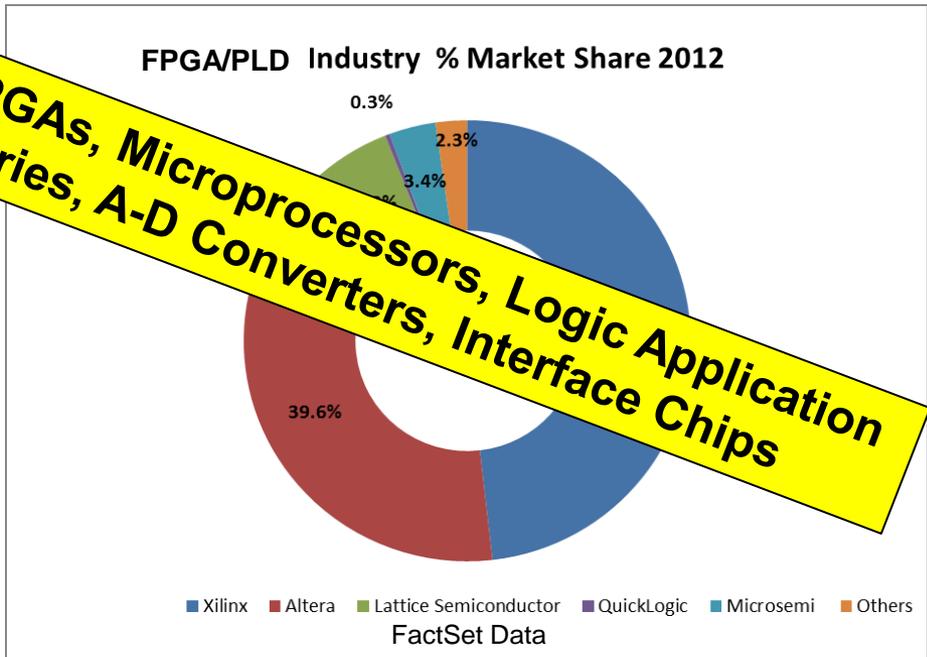
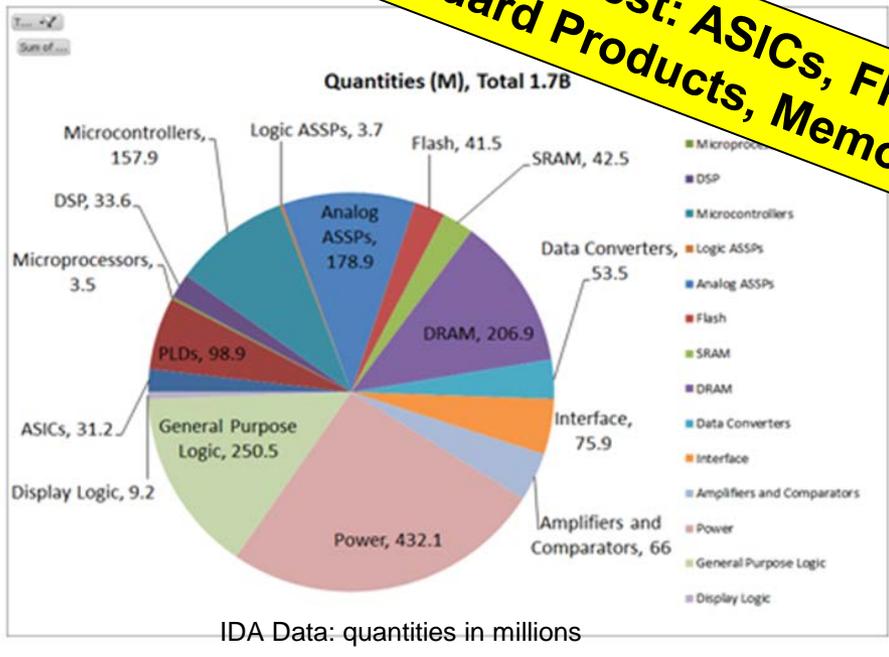


Identifying MicroE of Interest

Proposition: Focus trust policy on select devices

- Custom ASIC (57 vendors DMEA accredited)
- Hybrid (54 vendors QML approved by DLA for space apps)
- Custom/tailored FPGA (2 vendors have 88% of DoD market)
- ...Other ... selecting criteria *(developing mitigations w/DMEA)*

In general order of interest: ASICs, FPGAs, Microprocessors, Logic Application Specific Standard Products, Memories, A-D Converters, Interface Chips





Many Supply Chain Risks to Consider



Fraudulent Product

Counterfeit and other than genuine and new devices from the legally authorized source including relabeled, recycled, cloned, defective, out-of-spec, etc.

Malicious Insertion

The intentional insertion of malicious hard/soft coding, or defect to enable physical attacks or cause mission failure; includes logic bombs, Trojan 'kill switches' and backdoors for unauthorized control and access to logic and data

Anti-Tamper

Unauthorized extraction of sensitive intellectual property using reverse engineering, side channel scanning, runtime security analysis, embedded system security weakness, etc.

Quality Escape

Product defect/inadequacy introduced either through mistake or negligence during design, production, and post-production handling resulting in the introduction of deficiencies, vulnerabilities, and degraded life-cycle performance

Reliability Failure

Mission failure in the field due to environmental factors unique to military and aerospace environment factors such as particle strikes, device aging, hot-spots, electro-magnetic pulse, etc.

Emerging Threats

New threats, counterfeit trends, security attacks, and trust issues that combine two or more threats

Proposition: Risk Assessment approach must be integrated to address all

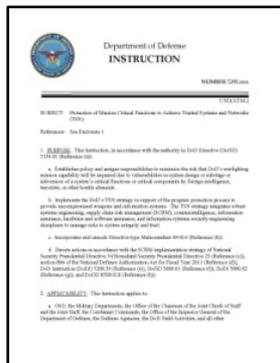


Program Protection Integrated Supply Chain Policy



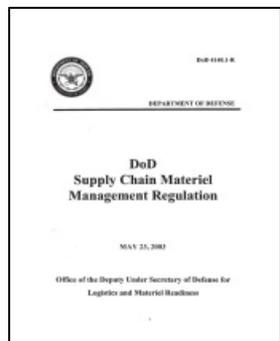
DoDI 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)

- 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, 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 stress conforming CAI to contract and technical requirements.



Proposition: Add security risk criteria to safety, reliability, etc. for Critical Application Items (CAI) designation in the supply chain to assist in managing MicroE CCs throughout the lifecycle



CAI aka CC List

- **During system development, contractor submits a proposed list of MicroE CCs that meet security risk criteria**
 - Subject to SE and/or Engineering Support Activity (ESA) approval and oversight
 - CAI designation for security necessitates trusted supply chain flow for ASICs and FPGAs (when practicable)
 - Provides candidate Level I and II CCs for Defense Intelligence Agency (DIA) Threat Assessment Center (TAC) assessments and requiring program protection countermeasures
- **Contractually require the MicroE CC list via special provision and CDRL**
 - SOW task and CDRL in RFP
 - Prime Contractor responsible for maintaining BOM and traceability flow down to suppliers in modular BOMs



Quality – Safety – Security Interrelationship



- **Analogous to Aviation Critical Safety Items (CSIs), MicroE are critical security risks if malicious code or a hidden defect can cause:**
 1. A catastrophic or critical failure resulting in the loss of or serious damage to a mission critical system;
 2. An unacceptable risk of personal injury or loss of life; or
 3. An uncommanded system failure jeopardizing safety or security.

Performance Specification: Integrated Circuits (Microcircuits) Manufacturing, General Specification for, MIL-PRF-38535K

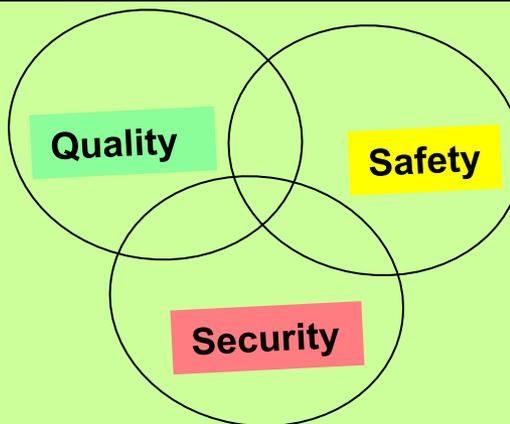
- General performance requirements for ICs
- Quality and reliability assurance requirements
- Requires manufacturer to establish a process flow baseline
- Provides certification and qualification criteria for manufacturer to be on Qualified Manufacturer List (QML).

Test Method Standard: Microcircuits, MIL-STD-883J

- Establishes methods/controls/procedures for testing
- Intended for Military and Aerospace electronic systems
- Controls/constraints to ensure quality and reliability

System Security Engineering Program Management Requirements, MIL-HDBK-1785

- Engineering out security vulnerabilities and designing in countermeasures for life-cycle security of critical defense resources
- Product Security Programs: Government outlines protection criteria for manufacturing critical components; contractor provides input



DoD Standard Practice: System Safety, MIL-STD-882E

- Hardware or software items
- Determined to potentially contribute to catastrophic or critical mishap
- May mitigate hazard with catastrophic or critical potential

Critical Items List, DI-RELI-80685

- Lists items with critical impact to reliability to contract end items; single point impact
- Developed for space/launch systems, but tailorable for other systems

Visit ASSIST Online, the official source for specifications and standards used by DoD:
<https://assist.dla.mil/online/start/index.cfm>



Federal Logistics Information System (FLIS)



WebFLIS
Federal Logistics Information System
WebFLIS Home

Web FLIS National Stock Number (NSN) Output Data

[Search again?](#)

NSN: 5962000575982
Item Name: MICROCIRCUIT ASSEMBLY
Query Type: PUBLIC
Date of query: 12/4/2013 3:52:04 PM

Criticality Code

Identification [Back to Top](#)

FIIG	INC	CRIT CD	II	RPD MRC	DMIL	DMIL INT CD	NIIN ASGMT	PMIC ADP	ESD EMI	HMIC	HCC
A458AD	33695	X	M	4	D	1	1967152	A	Q	N	

SCHEDULE B: 8542900000

ENAC:

TIUID Indicator: N

Supplier Status

Reference/Part Number [Back to Top](#)

REF/PN	CAGE CD	STAT	RNCC	RNVC	DAC	RNAAC	RNEC	RNSC	RNJC	SADC	HCC	MSDS
DN124550-1	98230	A	3	2	2	XN	1	D				
DN103772-1	98230	A	5	2	2	XN	1	D				

Item Control Reference

Management [Back to Top](#)

EFF DT	MOE	AAC	SOS	UI	UI PRICE	QUP	CIIC	SLC	REP	USC
2013274	DN	Y	NRP	EA	\$10.00	1	Z	Q	M	N
2013274	DN	Y	NRP	EA	\$10.00	1	Z	Q		I



A Modular BOM in Support of Risk Assessment



- A maintained engineered indentured BOM can be an important information source for identifying and managing critical MicroE
- Identifies the system's:
 - Mission critical functions
 - Logic Bearing Components (LBCs), (hardware (HW), firmware (FW) and software (SW))
 - Level I/II CCs proposed to be tracked as CAIs that are a subset of LBCs determined by assessing:
 - o System impact
 - o Source
 - o Whether an IC, hybrid, printed circuit board, etc.
 - o Whether specifically designed for military use
 - o Overall priority for protection

xxx board BOM list						REDACTED VERSION
Date: 19 Aug 2013						
Qty	Reference Designator	Item Description	Supplier	Supplier Part no.	Manufacturer	Manufacturer Part no.
11	R13, R12, R17, R18, R19, R22, R23, R24, R28, R32, R33	33R 1% 63mW SMT	RST	6-9197	Ziphay	W0233R0FKED
3	R1,R2,R3	10K 1% 100mW SMT	Fast-teck	Q-00172		
3	LED1,LED2,LED3	LED SMT 0603 Green	Nearnell	16060	Queendark	16708VGC-A
5	D1,D3,D4,D5,D6	1N41 High-speed diodes	Catser	7-1N4148-T/R	PXN	41478,113
3	IC11,IC12,IC14	Dual Operational Amplifier	Catser	5-LM258AM	Fairman Semiconductor	2587AM
1	IC13	EEPROM Memory256K (32K X 8) 150ns 28DIP	RST	6-3165	Btmel	28C275-15PU



BOMs and Parts Management Policy



- **DoD 4120.24-M, Defense Standardization Program, C3.2.4., Parts Management, requires program offices to have a parts management process that ... promotes the use of parts with acceptable performance, quality, & reliability**
- **MIL-STD-3018, *Parts Management*, and data item description DI-SDMP-81748, *Parts Management Plan*, make parts management a contract requirement**
 - When used with SD-19, *Parts Management Guide*, sets up a parts management process for prime contractors, suppliers and subcontractors and identifies an efficient part selection process
 - Details how/when the contractor submits initial and updated parts list(s) or BOMs to the Government
 - Addresses the detection, mitigation, and disposition of counterfeit parts:
 - Electronic, electrical, and mechanical parts are to be addressed
 - Use AS5553A, Anti-Counterfeit Standard, as guidance for electronic parts
 - Update to MIL-STD-3018 needed to address detection and mitigation of malicious code in CAIs
- **Also need contract provisions and DIDs to complete risk assessment**



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



Recommendations



Refine MicroE policy to address more than ASICs

- **Align and leverage other relevant policies**
 - CM, parts management, anti-counterfeit, anti-tamper, ...
 - Modify security and quality-focused policies, e.g., DLA QML and QPL, to also address MicroE security
- **Adopt CAI designation for security to identify Level I/II CCs**
 - Develop detailed criteria for selecting CCs from LBCs
 - Based on criticality analysis of MicroE type and end use
 - Treat as CM items early in acquisition for emphasis later in BOM and FLIS
 - Most effective way to obtain engineered-modular BOM information for MicroE
 - Narrowly focuses parts search and selection to minimize reporting
 - Use security CAIs designation to highlight CCs for enterprise-wide consideration of countermeasures across the lifecycle
 - DFAR needed to flow-down CC identification and reporting with industry
- **Continue work with DMEA and other stakeholders to identify a cost-effective, enterprise-wide mitigation approach for MicroE countermeasures beyond use of the Trusted Foundry for ASICs**



Systems Engineering: Critical to Defense Acquisition



Innovation, Speed, Agility
<http://www.acq.osd.mil/se>



Acronyms



AIA	Advanced Integrity Analysis
ASIC	Application -Specific Integrated Circuit
ASR	Alternative Systems Review
ASSIST	Acquisition Streamlining and Standardization Information System
BOM	Bill of Materials
CAI	Critical Application Item
CC	Critical component
CDRL	Contract Data Requirements List
CI	Configuration Items
CDR	Critical Design Review
CM	Configuration Management
COTS	Commercial Off-The-Shelf
CSI	Critical safety item
DAG	Defense Acquisition Guidebook
DIA	Defense Intelligence Agency
DID	Data Item Description
DLA	Defense Logistics Agency
DMEA	Defense MicroElectronics Activity
DMSMS	Diminishing Manufacturing Sources and Material Shortages
ESA	Engineering Support Activity
FRP	Full-Rate Production
FW	Firmware
FLIS	Federal Logistics Information System
FPGA	Field-programmable gate array
HW	Hardware

IC	Integrated circuit
ICT	Integrated Circuit Technology
IUID	Item Unique Identification
LBC	Logic-bearing component
MicroE	Microelectronics
NIIN	National Item Identification Number
OCM	Original Component Manufacturer
PDR	Preliminary Design Review
PPP	Program Protection Plan
QSLD	Qualified Supplier List of Distributors
QML	Qualified Manufacturer List
QPL	Qualified Products List
QTSL	Qualified Testing Supplier List
RA	Risk Assessment
RFP	Request for Proposal
SCRM	Supply chain risk management
SE	Systems Engineering
SFR	System Functional Review
SOW	Statement of Work
SRR	System Requirements Review
SW	Software
SwA	Software assurance
TAC	Threat Assessment Center
TDS	Technology Development Strategy
TNS	Trusted networks and systems



Web Resources



- **ASSIST Online, the source for DoD Standards, Specifications**
<https://assist.dla.mil/>
- **Defense Acquisition Guidebook**
<https://dag.dau.mil>
- **Defense MicroElectronics Activity (DMEA)**
<http://www.dmea.osd.mil/>
- **Defense Standardization Program**
<http://www.dsp.dla.mil/>
- **DoD Issuances (e.g., Directives, Instructions, Publications/Manuals)**
<http://www.dtic.mil/whs/directives/index.html>
- **Federal Logistics Information System (FLIS)**
<http://www.dlis.dla.mil/webflis/>
- **SAE**
<http://standards.sae.org/as5553a/>



MicroE-related Issuances and Guidance



- **DoDI 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)**
- **DoD 4140.1-R, DoD Supply Chain Materiel Management Regulation**
- **DoD 4140.26M DoD Integrated Materiel Management (IMM) for Consumable Items**
- **DoDI 4140.67 DoD Counterfeit Prevention Policy**
- **Defense Acquisition Guidebook Chapter 13, Program Protection Planning**



MicroE-related DIDs, Handbooks, Manuals, Specifications, and Standards



- **DI-RELI-80685, Critical Items List**
- **DI-SDMP-81748, Parts Management Plan**
- **DoD 4120.24-M, Defense Standardization Program**
- **MIL-HDBK-61A(SE), Configuration Management Guidance**
- **MIL-HDBK-1785, System Security Engineering Program Management Requirements**
- **MIL-PRF-38535K, Performance Specification: Integrated Circuits (Microcircuits) Manufacturing, General Specification for**
- **MIL-STD-882E, DoD Standard Practice: System Safety**
- **MIL-STD-883J, Test Method Standard: Microcircuits**
- **MIL-STD-3018, Parts Management**
- **SAE AS5553A, Fraudulent/Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition**
- **SD-19, Parts Management Guide**