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
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

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

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

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

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?
**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

- **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 CC Criteria
- Customer Needs
- Requirements

Life-Cycle Sustainment
- Organic Inventory Reassignment
- Contractor Logistic Support

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

Systems Engineering Process
- Reqmts Analysis
- Functional Analysis/Allocation
- Design Loop
- Verification
- Synthesis
- Reqmts Loop
- Outputs are Configuration Documentation
- Full Rate Production/Full Deployment Decision
- Parts Management

Configuration Management (CM) Process
- System Analysis & Control
- CM is Control Mechanism

Materiel Solution Analysis (MSA)
- Technology Maturation & Risk Reduction (TMRR)

Engineering & Manufacturing Development (EMD)
- Production & Deployment (P&D)

Full Rate Production/Full Deployment Decision
### Hardware Control (HC):

<table>
<thead>
<tr>
<th><strong>System-level:</strong> Establish initial HC criteria, critical functions and risk mitigation approach.</th>
</tr>
</thead>
</table>

**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.

**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.

**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.

### Supplier/Supply Chain Control (SC):

<table>
<thead>
<tr>
<th><strong>System-level:</strong> Establish initial SC criteria, critical functions and risk mitigation approach.</th>
</tr>
</thead>
</table>

**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.

**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.

**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.

---

* 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

Vulnerability & Threat Analysis

Increased Mitigation Investment

System Level Verification Test

Product Level Acceptance Test
DLA Qualified Testing Supplier List (QTSL)

Countermeasures selected based on Risk

AIA* Destructive Test
AIA* Nondestructive Test

Organic Foundry

Organic Design

DMEA Accredited Supplier**

DLA Qualified Manufacturer List (QML)

Qualified Supplier List of Distributors (QSLD)

Anti-Counterfeit Procedure & Inspections**

IUID** Traceability (DLA DNA, etc.)

Original Component Manufacturer (OCM)

OCM Authorized Distributor

Anonymity Procurement Practice

Commercial Practice

Criticality Analysis

Consequence for Life & Mission

* Advanced Integrity Analysis (AIA)
**DoD Instructions in Place
Transition from Configuration to Parts Management

Acquisition 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

Service Requirements

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

Logistics Reassignment Process

Sustainment Process

- Integrated Materiel Management
- Wholesale management of consumable items

DoD 4140.26M DoD Integrated Materiel Management (IMM) for Consumable Items
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)
- Semi-custom/tailored FPGA (2 vendors have 88% of DoD market)
- ... Other MicroEs meeting criteria (developing mitigations w/DMEA)

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

IDA Data: quantities in millions

FactSet Data
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

DoD Issuances Website: http://www.dtic.mil/whs/directives/corres/ins1.html
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 Interrelationships

- 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.

- 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

**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

**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

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)

Web FLIS National Stock Number (NSN) Output Data

<table>
<thead>
<tr>
<th>NSN</th>
<th>Item Name</th>
<th>Query Type</th>
<th>Date of query</th>
</tr>
</thead>
<tbody>
<tr>
<td>59620000575902</td>
<td>MICROCIRCUIT ASSEMBLY</td>
<td>PUBLIC</td>
<td>12/4/2013 3:52:04 PM</td>
</tr>
</tbody>
</table>

### Criticality Code

<table>
<thead>
<tr>
<th>Item</th>
<th>Code</th>
<th>Criticality</th>
</tr>
</thead>
<tbody>
<tr>
<td>A458A0 33695</td>
<td>X</td>
<td>M 4 D 1</td>
</tr>
<tr>
<td>8542900000</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Supplier Status

<table>
<thead>
<tr>
<th>Reference/Part Number</th>
<th>CAGE Code</th>
<th>Status</th>
<th>RNCC</th>
<th>RNVC</th>
<th>DAC</th>
<th>RNAAC</th>
<th>RNFC</th>
<th>RNSC</th>
<th>RNJC</th>
<th>SADC</th>
<th>HCC</th>
<th>MSDS</th>
</tr>
</thead>
<tbody>
<tr>
<td>ON124550-1</td>
<td>98230</td>
<td>A</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>XN</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ON103772-1</td>
<td>98230</td>
<td>A</td>
<td>5</td>
<td>2</td>
<td>2</td>
<td>XN</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Item Control Reference

<table>
<thead>
<tr>
<th>Reference/Part Number</th>
<th>EFF-DT</th>
<th>MOE</th>
<th>AAC</th>
<th>SOS</th>
<th>UI</th>
<th>UI PRICE</th>
<th>QUP</th>
<th>CIIC</th>
<th>SLC</th>
<th>REP</th>
<th>USC</th>
</tr>
</thead>
<tbody>
<tr>
<td>2013274</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2013274</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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:
    - System impact
    - Source
    - Whether an IC, hybrid, printed circuit board, etc.
    - Whether specifically designed for military use
    - Overall priority for protection

<table>
<thead>
<tr>
<th>Date: 19 Aug 2013</th>
<th>Redacted Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Qty</td>
<td>Reference Designator</td>
</tr>
<tr>
<td>11</td>
<td>R13, R12, R17, R18, R19, R22, R23, R24, R28, R32, R33</td>
</tr>
<tr>
<td>3</td>
<td>R1,R2,R3</td>
</tr>
<tr>
<td>3</td>
<td>LED1,LED2,LED3</td>
</tr>
<tr>
<td>5</td>
<td>D1,D3,D4,D5,D6</td>
</tr>
<tr>
<td>5</td>
<td>IC11,IC12,IC14</td>
</tr>
<tr>
<td>1</td>
<td>IC13</td>
</tr>
</tbody>
</table>
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

- 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

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIA</td>
<td>Advanced Integrity Analysis</td>
</tr>
<tr>
<td>ASIC</td>
<td>Application-Specific Integrated Circuit</td>
</tr>
<tr>
<td>ASR</td>
<td>Alternative Systems Review</td>
</tr>
<tr>
<td>ASSIST</td>
<td>Acquisition Streamlining and Standardization Information System</td>
</tr>
<tr>
<td>BOM</td>
<td>Bill of Materials</td>
</tr>
<tr>
<td>CAI</td>
<td>Critical Application Item</td>
</tr>
<tr>
<td>CC</td>
<td>Critical component</td>
</tr>
<tr>
<td>CDRL</td>
<td>Contract Data Requirements List</td>
</tr>
<tr>
<td>CI</td>
<td>Configuration Items</td>
</tr>
<tr>
<td>CDR</td>
<td>Critical Design Review</td>
</tr>
<tr>
<td>CM</td>
<td>Configuration Management</td>
</tr>
<tr>
<td>COTS</td>
<td>Commercial Off-The-Shelf</td>
</tr>
<tr>
<td>CSI</td>
<td>Critical safety item</td>
</tr>
<tr>
<td>DAG</td>
<td>Defense Acquisition Guidebook</td>
</tr>
<tr>
<td>DIA</td>
<td>Defense Intelligence Agency</td>
</tr>
<tr>
<td>DID</td>
<td>Data Item Description</td>
</tr>
<tr>
<td>DLA</td>
<td>Defense Logistics Agency</td>
</tr>
<tr>
<td>DMEA</td>
<td>Defense MicroElectronics Activity</td>
</tr>
<tr>
<td>DMSMS</td>
<td>Diminishing Manufacturing Sources and Material Shortages</td>
</tr>
<tr>
<td>ESA</td>
<td>Engineering Support Activity</td>
</tr>
<tr>
<td>FRP</td>
<td>Full-Rate Production</td>
</tr>
<tr>
<td>FW</td>
<td>Firmware</td>
</tr>
<tr>
<td>FLIS</td>
<td>Federal Logistics Information System</td>
</tr>
<tr>
<td>FPGA</td>
<td>Field-programmable gate array</td>
</tr>
<tr>
<td>HW</td>
<td>Hardware</td>
</tr>
<tr>
<td>IC</td>
<td>Integrated circuit</td>
</tr>
<tr>
<td>ICT</td>
<td>Integrated Circuit Technology</td>
</tr>
<tr>
<td>IUID</td>
<td>Item Unique Identification</td>
</tr>
<tr>
<td>LBC</td>
<td>Logic-bearing component</td>
</tr>
<tr>
<td>MicroE</td>
<td>Microelectronics</td>
</tr>
<tr>
<td>NIIN</td>
<td>National Item Identification Number</td>
</tr>
<tr>
<td>OCM</td>
<td>Original Component Manufacturer</td>
</tr>
<tr>
<td>PDR</td>
<td>Preliminary Design Review</td>
</tr>
<tr>
<td>PPP</td>
<td>Program Protection Plan</td>
</tr>
<tr>
<td>QSLD</td>
<td>Qualified Supplier List of Distributors</td>
</tr>
<tr>
<td>QML</td>
<td>Qualified Manufacturer List</td>
</tr>
<tr>
<td>QPL</td>
<td>Qualified Products List</td>
</tr>
<tr>
<td>QTSL</td>
<td>Qualified Testing Supplier List</td>
</tr>
<tr>
<td>RA</td>
<td>Risk Assessment</td>
</tr>
<tr>
<td>RFP</td>
<td>Request for Proposal</td>
</tr>
<tr>
<td>SCRIM</td>
<td>Supply chain risk management</td>
</tr>
<tr>
<td>SE</td>
<td>Systems Engineering</td>
</tr>
<tr>
<td>SFR</td>
<td>System Functional Review</td>
</tr>
<tr>
<td>SOW</td>
<td>Statement of Work</td>
</tr>
<tr>
<td>SRR</td>
<td>System Requirements Review</td>
</tr>
<tr>
<td>SW</td>
<td>Software</td>
</tr>
<tr>
<td>SwA</td>
<td>Software assurance</td>
</tr>
<tr>
<td>TAC</td>
<td>Threat Assessment Center</td>
</tr>
<tr>
<td>TDS</td>
<td>Technology Development Strategy</td>
</tr>
<tr>
<td>TNS</td>
<td>Trusted networks and systems</td>
</tr>
</tbody>
</table>
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)

• 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-STD-882E, DoD Standard Practice: System Safety
- MIL-STD-3018, Parts Management
- SAE AS5553A, Fraudulent/Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition
- SD-19, Parts Management Guide