G-12 Space Subcommittee - Space Concerns

Distinguished Engineer
The Aerospace Corporation
Electronics and Sensors Division / Engineering & Technology Group

Branch Chief – Mission Assurance
The Aerospace Corporation
Imagery Products Division / National Systems Group

January 14, 2014

© The Aerospace Corporation 2013

Topics

- DLA Supplier Audits
- Participation in G-12/G-11 Meetings
- MIL-PRF-38535 Concerns
- MIL-STD-1580
- TRUSTED Supply Chain

DLA Supplier Audits

- Based on reduced funding limitations, Aerospace will participate in DLA audits, but at a limited effort
- "The Aerospace Corporation" (Aerospace) is generating a list of priority audits important to the space community and will work with DLA to ensure coverage
- Members of the space contractor community should contact Aerospace for any audits they deem important or critical

Participation in JEDEC/G-12/G-11 Meetings

- "The Aerospace Corporation's" (Aerospace) Support to JEDEC/G-12/G-11 Meetings are important to the understanding of industry issues and resolution for space
  - Overall Government funding has been reduced
    - Aerospace is working with SMC and programs to ensure funding availability
  - Aerospace will support the meetings as required
    - The agenda for each meeting will be reviewed and the resources necessary will be employed to cover all areas of technical expertise

MIL-PRF-38535 Concerns

- MIL-PRF-38535 Rev K released
- Class Y now invoked but some areas of concern still exist (being worked by task groups
  - *TM 5011 relative to underfill*
    - TM 5011 was intended to cover outgassing on the underfill but Aerospace had previously brought up an evaluation of the underfill stability for long term
  - *BME capacitors*
- Radiation testing
  - *Off-shore suppliers who are QML Class V and rad hard have encountered some issues relative to ITAR and testing and providing data*
    - Potential for DLA to approve off-shore rad facility

MIL-STD-1580

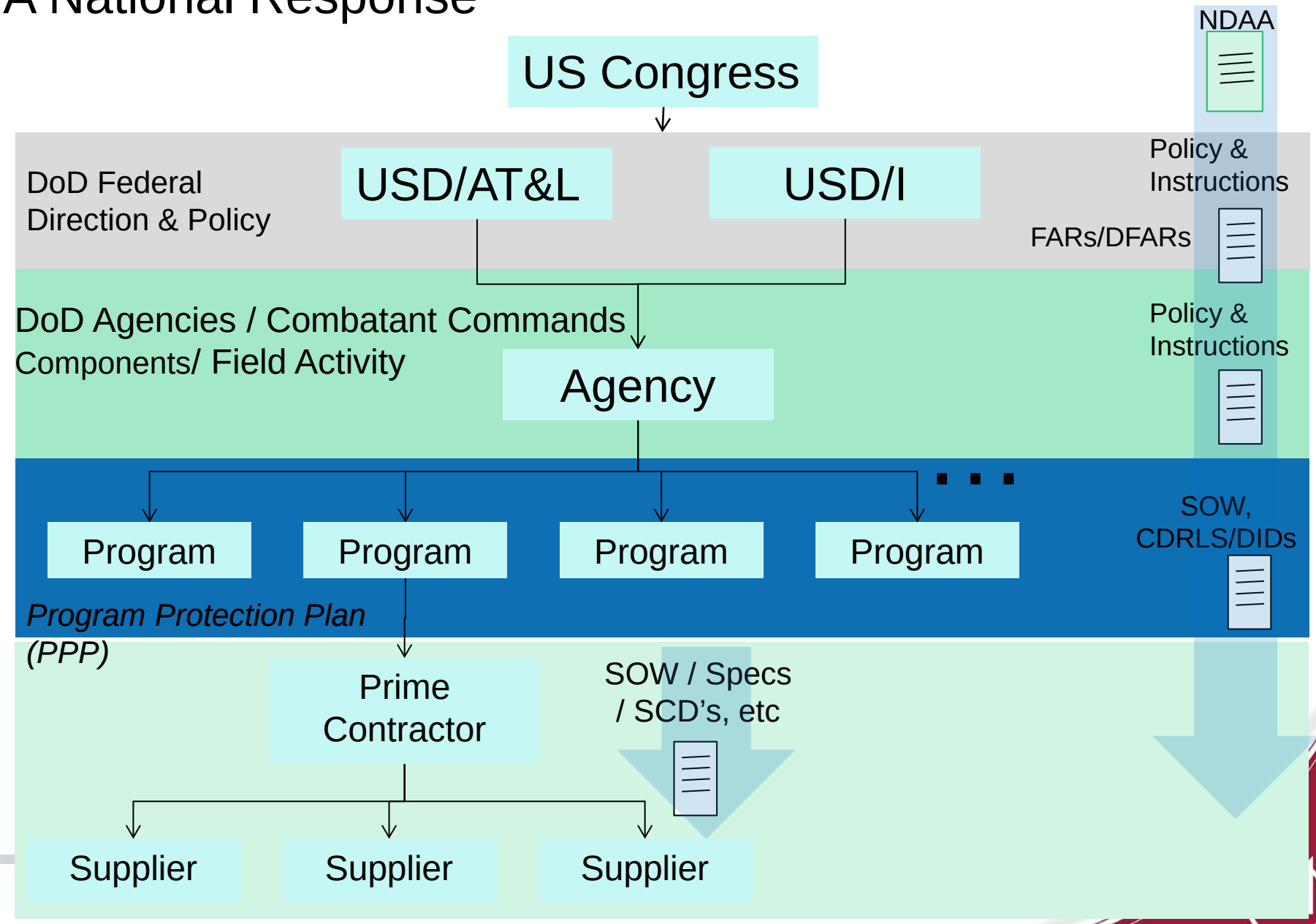
- Previous discussions at JEDEC have centered on the need to modify DPA requirements in MIL-STD-1580
- Overall Government budgets have been reduced and a priority to work changes to this document need to be evaluated
- Some information of potential changes have been identified but no formal combined list of issues/changes has been presented
- DLA published a draft of changes to some of the resistor sections. Aerospace nor the space community were aware of these changes being considered. WHO WAS THE AUTHOR & WHY DID THEY NOT COME THROUGH THE TASK GROUP

AEROSPACE
Assuring Space Mission Success

Program Protection Planning for Supply Chain Risk Management and Prevention and Mitigation of Counterfeit, Fraudulent and Malicious Parts and Materials

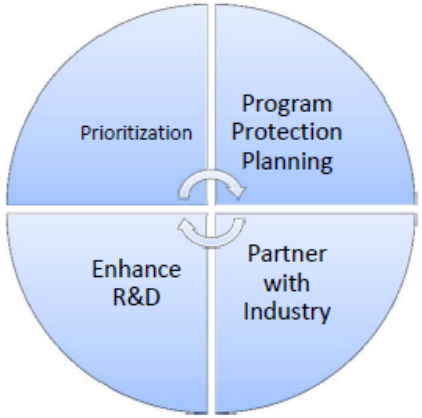
© The Aerospace Corporation 2013

A National Response



Trusted Defense Systems Strategy: Basic Tenets

- **Prioritization:**
  - Focus security requirements on mission critical systems
  - Within systems, identify and protect critical components, technology, information
- **Comprehensive Program Protection Planning**
  - Early lifecycle identification of trusted and critical components
  - Provide PMs with criticality analysis of supply chain risk
  - Protect critical components through trusted suppliers, or secure systems design
  - Assure systems through advanced vulnerability detection, test and evaluation
  - Manage counterfeit risk through sustainment
- **Partner with Industry**
  - Develop commercial standards for secure products
- **Enhance capability through R&D**
  - Leverage and enhance automated vulnerability detection tools and capabilities for software
  - Technology investment to advance secure software, hardware, and system design methods



Distribution Statement A – Approved for public release by OSR; SR# 13-S-1385 and 13-S-2291 apply. Distribution is unlimited.

Why the Focus on Trusted Systems?

- ***Threat*: Nation-state, terrorist, criminal, or rogue developer who:**
  - Gain control of systems through supply chain opportunities
  - Exploit vulnerabilities remotely
- ***Vulnerabilities***
  - All systems, networks, and applications
  - Lack of SCRM
  - Intentionally implanted logic
  - Unintentional vulnerabilities maliciously exploited (e.g., poor quality or fragile code)
- ***Traditional Consequences*: Loss of critical data, technology or capability**
- ***Emerging Consequences*: Loss of manufacturing technology, intellectual property and 'know how'**
- **All can result in loss of critical warfighting capability**

Today's acquisition environment paradigm change has introduced new vulnerabilities:

Stand-alone systems	>>>	Networked systems
Some software functions	>>>	Software-intensive
Known supply base	>>>	Prime Integrator, hundreds of suppliers
CPI (technologies)	>>>	CPI and critical components

Distribution Statement A – Approved for public release by OSR; SR# 13-S-1385 and 13-S-2291 apply. Distribution is unlimited.

What Are We Protecting?

Program Protection Planning

DoDI 5000.02

DoDI 5200.39	DoDI 5200.44	DoDI 8500 Series DoDI 8582.01
Technology	**Components**	**Information**
What: Leading-edge research and technology **Who Identifies**: Technologists, System Engineers **ID Process**: CPI Identification **Threat Assessment**: Foreign collection threat informed by Intelligence and Counterintelligence assessments **Countermeasures**: AT, Classification, Export Controls, Security, Foreign Disclosure, and CI activities **Focus**: "Keep secret stuff in" by protecting any form of technology	**What**: Mission-critical elements and components **Who Identifies**: System Engineers, Logisticians **ID Process**: Criticality Analysis **Threat Assessment**: DIA SCRM TAC **Countermeasures**: SCRM, SSE, Anti-counterfeits, software assurance, Trusted Foundry, etc. **Focus**: "Keep malicious stuff out" by protecting key mission components	**What**: Information about applications, processes, capabilities and end-items **Who Identifies**: All **ID Process**: CPI identification, criticality analysis, and classification guidance **Threat Assessment**: Foreign collection threat informed by Intelligence and Counterintelligence assessments **Countermeasures**: Information Assurance, Classification, Export Controls, Security, etc. **Focus**: "Keep critical information from getting out" by protecting data

Protecting Warfighting Capability Throughout the Life Cycle

Distribution Statement A – Approved for public release by OSR; SR# 13-S-1385 and 13-S-2291 apply. Distribution is unlimited.

Program Protection Integrated in Policy

DoDI 5000.02 Operation of the Defense Acquisition System

- Regulatory Requirement for Program Protection Plan at Milestones A, B, C and FRP/FDD
- References DoDI 5200.39

DoDI 5200.39 Critical Program Information (CPI) Protection Within the DoD

- Assigns responsibility for Counterintelligence, Security, and System Engineering support for the ID and protection of CPI
- Expands definition of CPI to include degradation of mission effectiveness

DoDI 5200.44 Protection of Mission Critical Functions to Achieve Trusted Systems and Networks

- Establishes policy and responsibilities to minimize the risk that warfighting capability will be impaired due to vulnerabilities in system design or subversion of mission critical functions or components

DoDI 8500.01E Information Assurance

- Establishes policy and assigns responsibilities to achieve DoD information assurance (IA) through a defense-in-depth approach that integrates the capabilities of personnel, operations, and technology, and supports the evolution to network centric warfare

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

Distribution Statement A – Approved for public release by OSR; SR# 13-S-1385 and 13-S-2291 apply. Distribution is unlimited.

Program Protection Guidance

Program Protection Plan Outline & Guidance, dated 18 Jul 2011

- **Focal point for documenting Program security activities, including:**
  - Plans for identifying and managing risk to CPI and critical functions and components
  - Responsibilities for execution of comprehensive program protection
  - Tables of actionable data, not paragraphs of boilerplate
  - End-to-end system analysis and risk management
- **http://www.acq.osd.mil/se/docs/PPP-Outline-and-Guidance-v1-July2011.pdf**

Defense Acquisition Guidebook Chapter 13, "Program Protection"

- **Provides implementation guidance for TSN Analysis and CPI Protection**
- **Describes SSE activities throughout the Defense Acquisition Life Cycle**
- **https://acc.dau.mil/dag13**

Distribution Statement A – Approved for public release by OSR; SR# 13-S-1385 and 13-S-2291 apply. Distribution is unlimited.

Key Elements of the PPP

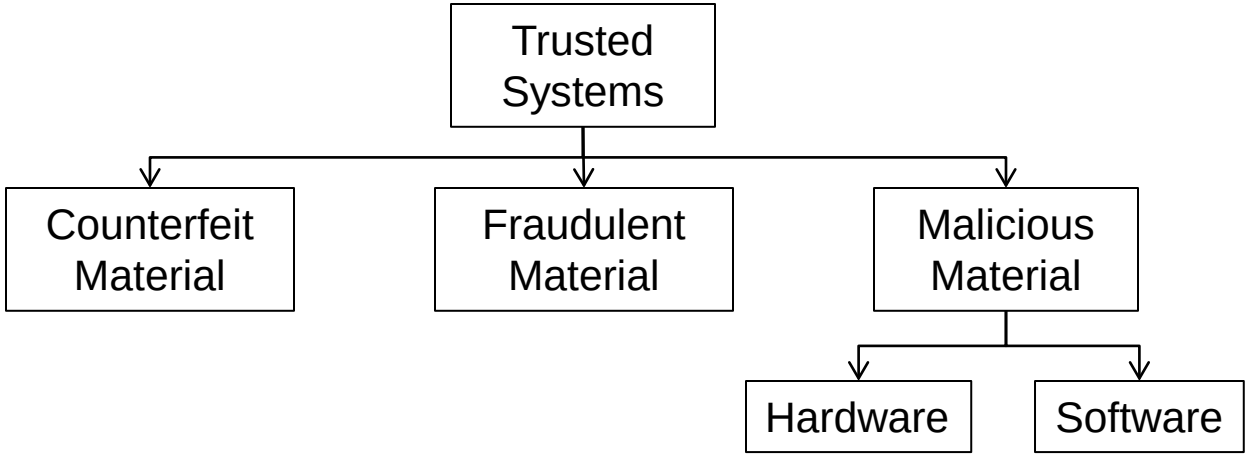
Key Sections	Rationale
3.0 CPI and Critical Components (CC) – Documents output of Research & Tech. Protect and Criticality Analysis – Distinguishes between inherited and organic elements	**Focus protection on critical technology, information, and components**
4.0 Horizontal Protection – Assessment of similar CPI on other DoD programs	**Protect technologies across the DoD**
5.0 Threats, Vulnerabilities and Countermeasures – Identifies collection, supply chain, and battlefield threats – Documents assessment of vulnerability to threats and mitigating actions	**Acknowledge advanced, persistent threat** **Assess weaknesses to documented threats and use risk-based mitigations**
6.0 Other Plans – Pointers to related documents (CI Support Plan, TEMP, etc.)	**Reference, not duplicate, key documents**
7.0 Residual Risk Assessment – Document unmitigated risks to CPI and CC compromise	**Document risks program is assuming**
8.0 Foreign Involvement – Identify known and potential foreign military sales, and direct commercial sales – Defense Exportability Features (DEF) opportunities	**Drive export realism and prepare for export-specific measures early**
9.0 Processes for PM Oversight & Implementation	**PM Resources and Implementation Reviews**
10.0 Processes for Monitoring & Reporting Loss of CPI and CC	**Assess effectiveness of implemented countermeasures**
11.0 Costs – Estimate of implementation costs for CPI and CC protection	**Support cost/benefit assessment of risk mitigations**

The PPP Contains the Information a PM Needs to Effectively Secure the System

Distribution Statement A – Approved for public release by OSR; SR# 13-S-1385 and 13-S-2291 apply. Distribution is unlimited.

Supply Chain Risk Management –Preventing Bad Actors

New DoD Instructions for ensuring Trusted Systems



USD (AT&L) issued new directives to prevent counterfeit and malicious hardware and software into ALL DoD Systems

- DoD I-4140.67 DoD Counterfeit Prevention Policy
- DoD I-5200.39 Critical Program Information (CPI) Protection within the DoD
- DoD I-5200.44 Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)
- IC Directive 731 Supply Chain Risk Management
- New FAR/DFAR Clauses and NDAA 2012, 2013 and 2014 sections

DoD I 5200.44 Trusted Systems and Networks

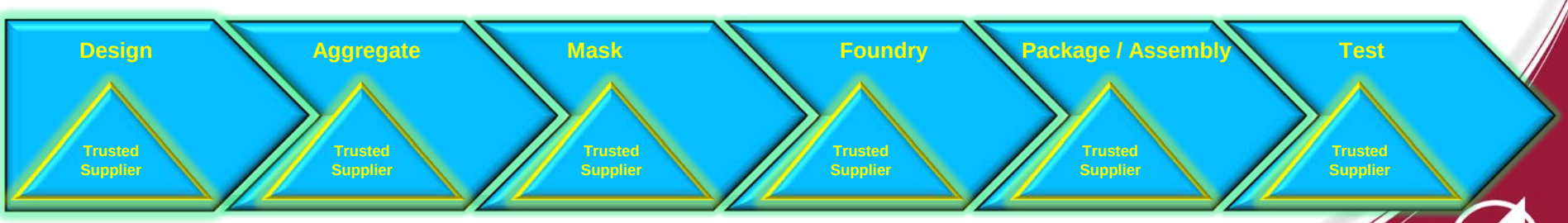
DoD Instruction 5200.44 requires that:

- 4.c.2 “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., integrated circuits, field-programmable gate arrays (FPGA), printed circuit boards) when they are identifiable (to the supplier) as having a DoD end-use. “
- 4.e “In applicable systems, integrated circuit-related products and services shall be procured from a trusted supplier accredited by the Defense Microelectronics Activity (DMEA) when they are custom-designed, custom-manufactured, or tailored for a specific DoD military end use (generally referred to as application-specific integrated circuits (ASIC)). “
- 1.g “In coordination with the DoD CIO, the Director, Defense Intelligence Agency (DIA), and the Heads of the DoD Components, 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 I-5200.44 is one part of the DoD’s overall implementation strategy to prevent counterfeit materials from entering the DoD Supply chain. See DoD I-4140.67 – DoD Counterfeit Prevention Policy

What 5200.44 Will mean to Programs

- Will need to assess and manage the supply chain risk for components in Critical Functions
  - *Integrated Circuits (ASICs)*
  - *Field Programmable Gate Arrays (FPGAs)*
  - *Printed Circuit Boards*
- Will need to assess the risk from counterfeits to Critical Functions and develop a plan to mitigate and manage those risks (above and beyond 4140.67)
- Will need to identify ASICs in Critical Functions and procure them through a Trusted Supply Chain either through
  - *Trusted Access Program Office (NSA – Fort Meade, MD)*
  - *Or directly from the Trusted supplier (Aeroflex, BAE Manassas, Honeywell, etc.)*



From: Dr. Brian Cohen, IDA

Policy and Guidance for ASICs

- PPP Outline and Guidance on Microelectronics for ASICs
  - *Requires programs to identify all ASICs that require an accredited trusted supplier*
  - *Requires program to describe how they will make use of accredited trusted suppliers of integrated circuit-related services*
- Defense Acquisition Guidebook (DAG) guidance (Chapter 13)
  - *ASICs meeting policy conditions must be procured from a DMEA accredited trusted supplier implementing a trusted product flow*
  - *Defense Microelectronics Activity (DMEA) maintains a list of accredited suppliers on its website at*
  - *http://www.dmea.osd.mil/trustedic.html.*
  - *Critical Design Review (CDR) criteria: Assess manufacturability including the availability of accredited suppliers for secure fabrication of Application-specific integrated circuits (ASICs), Field Programmable Gate Array (FPGAs), and other programmable devices*

- ***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;

Counterfeit PM&P Components - Definition

FAR/DFAR 48 CFR 202.101

- *Counterfeit part means—*
  - *(1) An unauthorized copy or substitute part that has been identified, marked, and/or altered by a source other than the part's legally authorized source and has been misrepresented to be from a legally authorized source;*
  - *(2) An item misrepresented to be an authorized item of the legally authorized source; or*
  - *(3) A new, used, outdated, or expired item from a legally authorized source that is misrepresented by any source to the end-user as meeting the performance requirements for the intended use.*
- *Legally authorized source means –*
  - *The current design activity or the original manufacturer or a supplier authorized by the current design activity or the original manufacturer to produce an item.*
- *Suspect counterfeit part means –*
  - *A part for which visual inspection, testing, or other information provide reason to believe that a part may be a counterfeit part.*

Examples of Counterfeit Parts include but not limited to:

- Parts which do not contain the proper internal construction (die, manufacturer, wire bonding, etc.) consistant with the ordered part
- Parts which have been used, refurbished or reclaimed, but represented as new product
- Parts which have different package style or surface plating/finish than the ordered parts
- Parts which have not successfully completed the OCM's full production run and test flow, but are represented as completed product
- Parts sold as upscreened parts, which have not successfully completed upscreening
- Parts sold with modified labeling or markings intended to misrepresent the part's form, fit, function or grade
- A part with a hidden feature that is intentionally introduced into the supply chain that has a malicious intent (e.g., well hidden feature, if activated, will render the host system inoperative).

Counterfeit Parts – Occurrence Procedures

If a counterfeit part or material is discovered in either receiving inspection or in inventory the contractor need to implement the following procedure:

Actions by the contractor:

1. Quarantine the parts; place them in bonded stores
2. Do <u>not notify</u> the supplier/vendor that they are suspected of selling counterfeit parts/materials
3. Notify the government contracting officer and/or the prime contractor's contract officer of the suspected counterfeit item.
4. Assemble a data package that contains a copy of the purchase order and, procurement specifications (source control drawing, specification), receiving inspection reports, copies of all correspondence (e-mails, telephone conversation notes, faxes) etc.
5. Deliver the suspected counterfeit items in accordance with the instructions received from the government or prime contractor's contracting officer.
6. Support the government's investigation as required

Actions to be taken by the government:

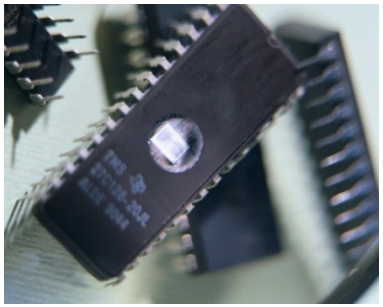
1. Travel to the contractors' facility to inspect / verify the counterfeit items
2. Notify the Office of the Inspector General of the counterfeit items
3. Provide instructions to the contractor on whom and where to deliver the counterfeit items and supporting data package
4. Perform an independent analysis (destructive physical analysis) on the suspected counterfeit items
5. Provide the counterfeit items, supporting data package and independent test results to the Office of the Inspector General to support their legal investigations.

Malicious Parts and Software

- Malicious means:
  - *An item (electrical/electronic part or software) that contains an embedded feature that was NOT designed-in by the authorized design activity, that could implement unwanted functionality into the operation of the part or software*
- Examples include:
  - *Phone home capability in Laptop or Desktop computers*
  - *"Kill Switch"*
  - *Erroneous data generation*
    - Timing signals
    - Corrupted data
- How does it get into our systems
  - *Foreign intrusion into unprotected systems*
  - *Use of open software downloaded from the internet*
  - *Intentional sabotage*

Proposition: Trust Policy Objective

- Implement Supply Chain Risk Management (SCRM) on MicroE components used in National Security Systems when military end use 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 components of interest include, but are not limited to:
  - *Define a sequence of instructions,*
  - *Perform one or more decision making functions,*
  - *Execute basic units of logic,*
  - *Or can be surreptitiously altered to trigger malicious functionality or the loss of confidential information.*



- Examples of MicroE that may be critical include vulnerable custom ASICs, program logic devices (FPGA), micro-processors, Application Specific Standard Products, and flash memory

How do we find them and mitigate the risk?

Problem Statement

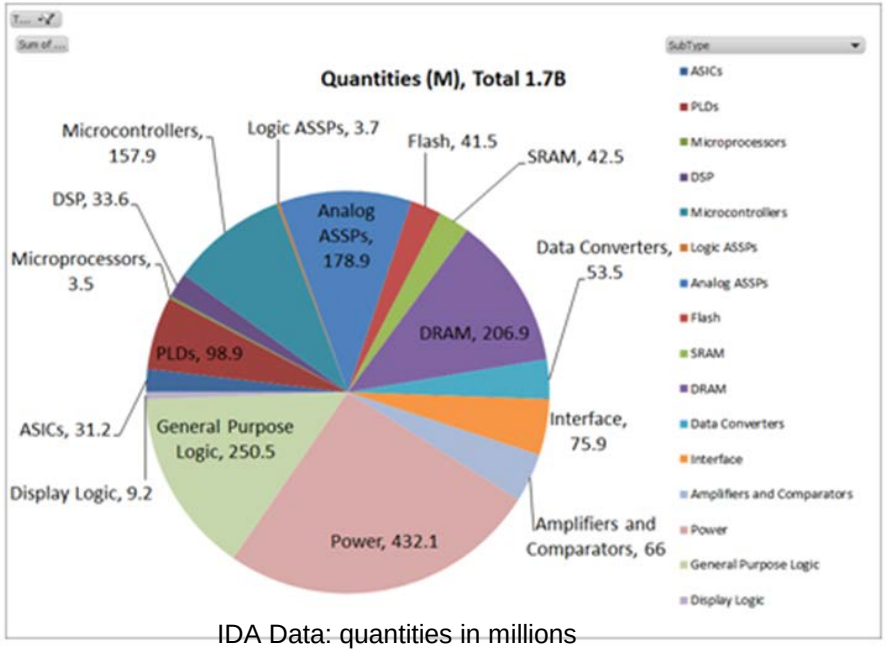
Vulnerabilities in supply chain could lead to malicious logic insertions

- 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)

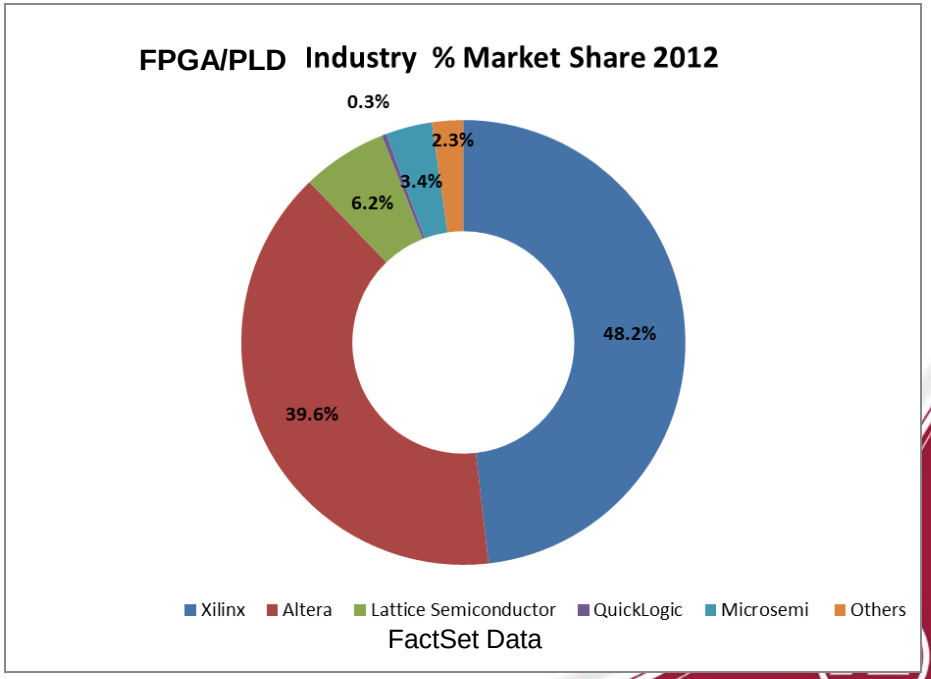
Identifying MicroE of Interest

Proposition: Focus trust policy on select devices

- Custom ASIC (57 DMEA Accredited)
- Hybrid (54 QML approved by DLA for Space Apps)
- Semi-custom/tailored FPGA (2 have 88% of DoD market)
- …other MicroE meeting criteria *(developing mitigations w/DMEA)*



IDA Data: quantities in millions



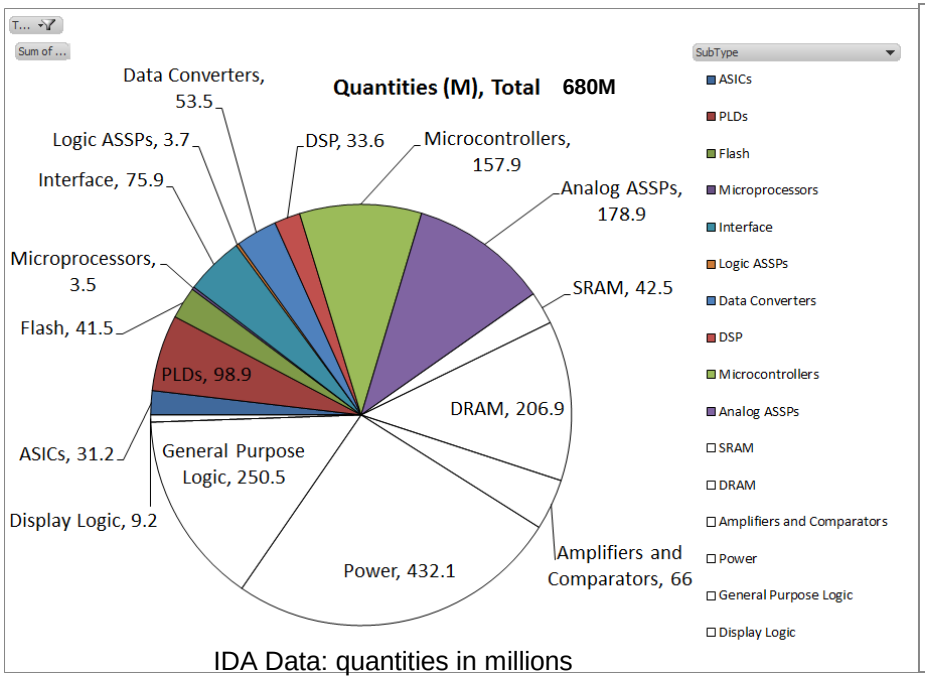
FactSet Data

Identifying MicroE of Interest

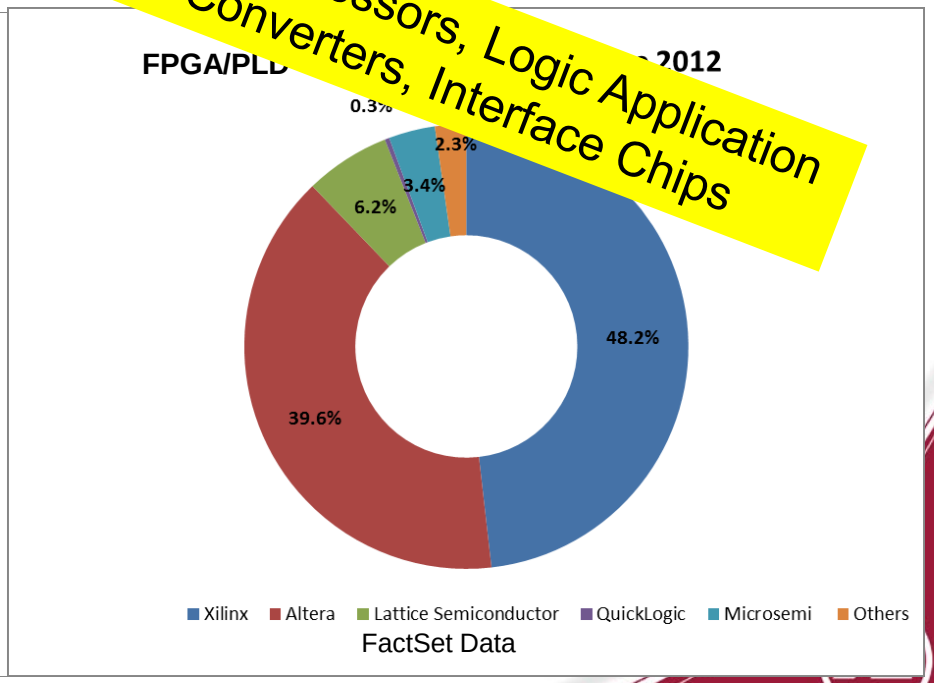
Proposition: Focus trust policy on select devices

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

- Custom A[illegible] Accredited)
- Hybrid (54 QML a[illegible] A for Space Apps)
- Semi-custom/tailored FP[illegible] of DoD market)
- …other MicroE meeting the criteri[illegible] *[illegible]tigations w/DMEA)*

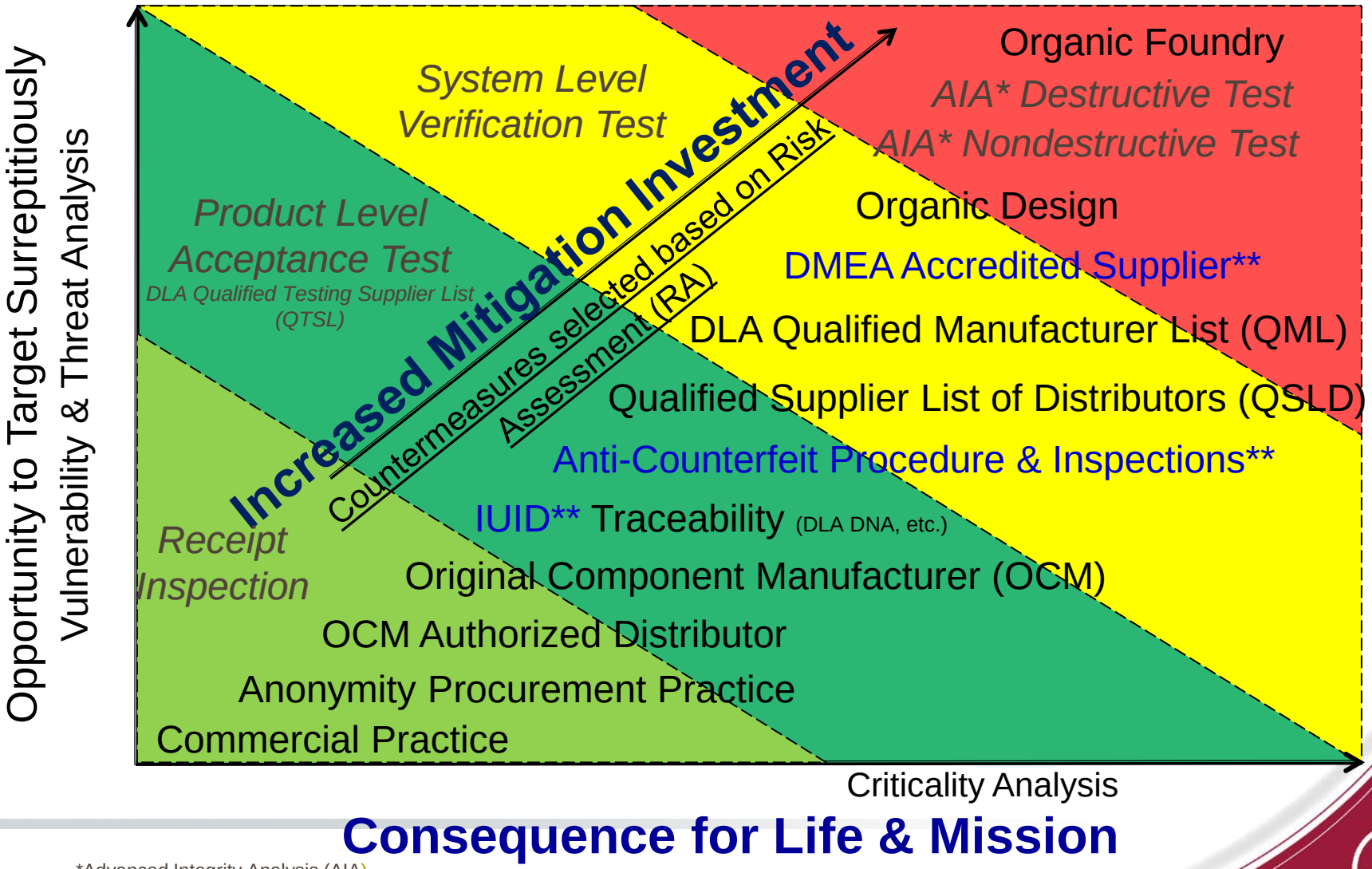


IDA Data: quantities in millions



FactSet Data

Supply Chain Risk Countermeasures



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

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: RA approach must be integrated to address all

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

TRUSTED Supply Chain

- Presidential order DoDI 5200.44 signed Nov 2012 requiring all DoD efforts incorporation FPGAs and ASICs to be procured through a “TRUSTED” Supply Chain
- “TRUSTED” implies certification and approval through DMEA
- Need to incorporate “TRUSTED” into MIL-PRF-38535

AEROSPACE
Assuring Space Mission Success

Thank you

© The Aerospace Corporation 2013

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)