



**U.S. ARMY**  
**RDECOM**

*AMRDEC Counterfeit  
Risk Management  
Recommendations*

Approved for public release; distribution unlimited.  
Review completed by the AMRDEC Public Affairs  
Office 29 Aug 2013; PR0033..



**TECHNOLOGY DRIVEN. WARFIGHTER FOCUSED.**

**August 2013**

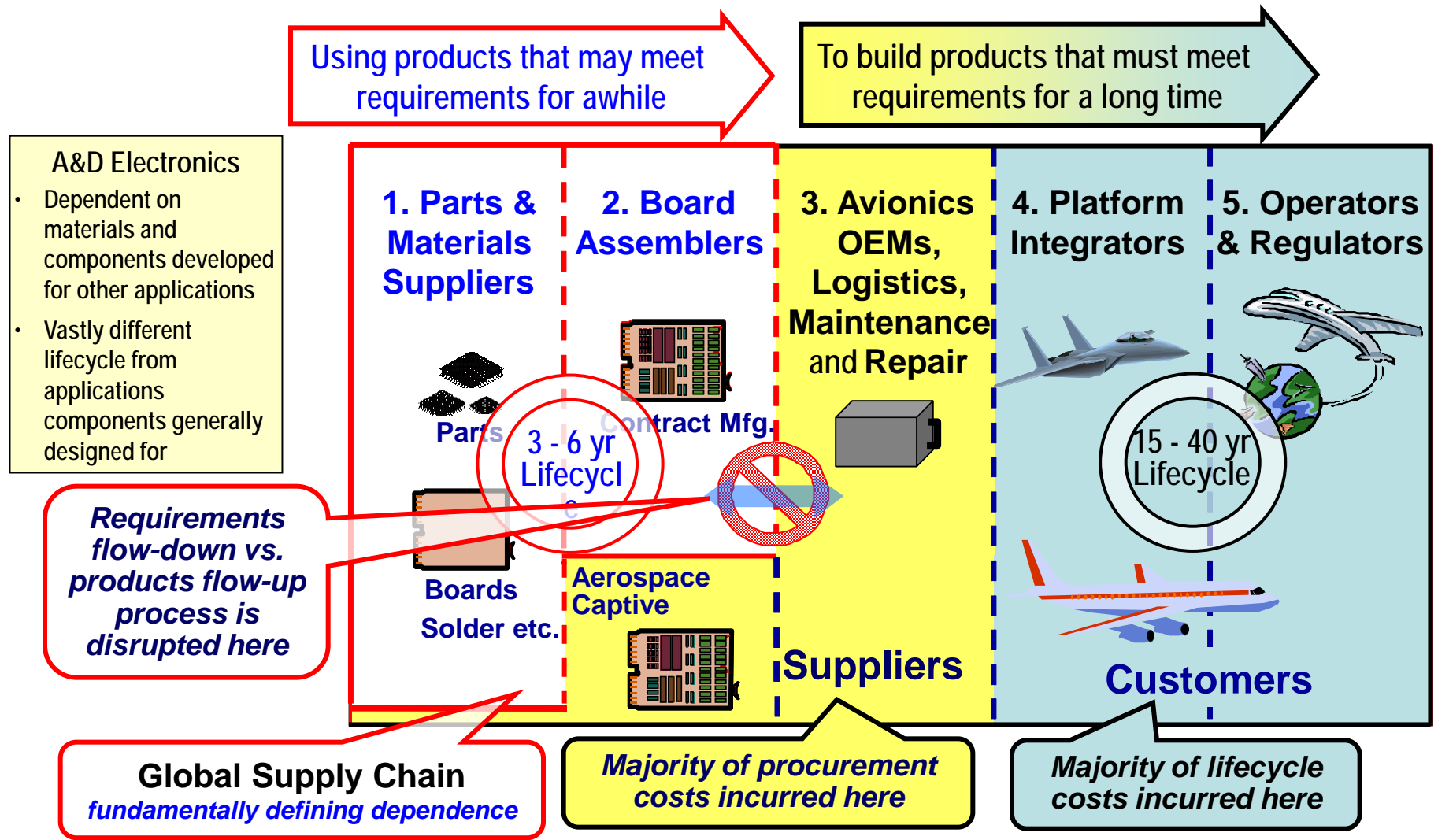
*Presented by:*

**David Locker**

**David.Locker@us.army.mil (256-842-0163)**

**Engineering Directorate**


**U.S. Army Aviation and Missile Research,  
Development, and Engineering Center**



- **Counterfeit**
  - Any materiel whose identity or pedigree has been ***deliberately altered, misrepresented*** or offered as an ***unauthorized product substitution***
  - Could be as simple as re-marking scrapped or stolen and possibly nonworking parts, or as complex as illegally manufacturing complete parts from original molds or designs.
  - Obsolete components are not the only parts being counterfeited – there are also counterfeit versions of the newest parts and components currently being manufactured by Original Component Manufacturers (OCM)
- **Reasons for Counterfeit Occurrences and Risk**
  - Two major challenges facing the U.S. military services
    1. **Extension of weapon systems and platform lifecycles**
    2. **Sustainment of the aging systems**
  - Less expensive to find part substitutions and aftermarket manufacturing for needed electronic parts than reengineering and redesigning parts and components
  - Defense electronics represents only about 1% of market place, resulting in **long lead times** for many parts that meet defense requirements (e.g., temp range and lead finishes)

- **Types of Common Counterfeits**

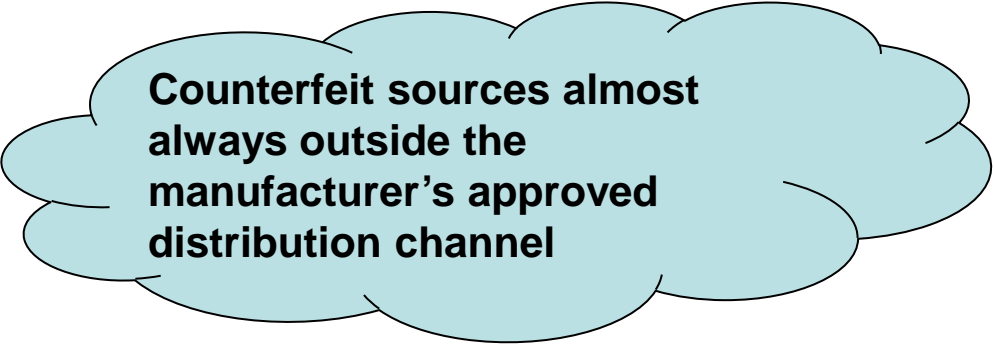
- Used / New Product Re-Marked as Higher Grade New Product
- Used Product Sold as New (Not Remarketed)
- Invalid Part Marking
- Fake Non-Working Product



**Counterfeit Impact:  
Reduced System  
Performance and  
Reliability**

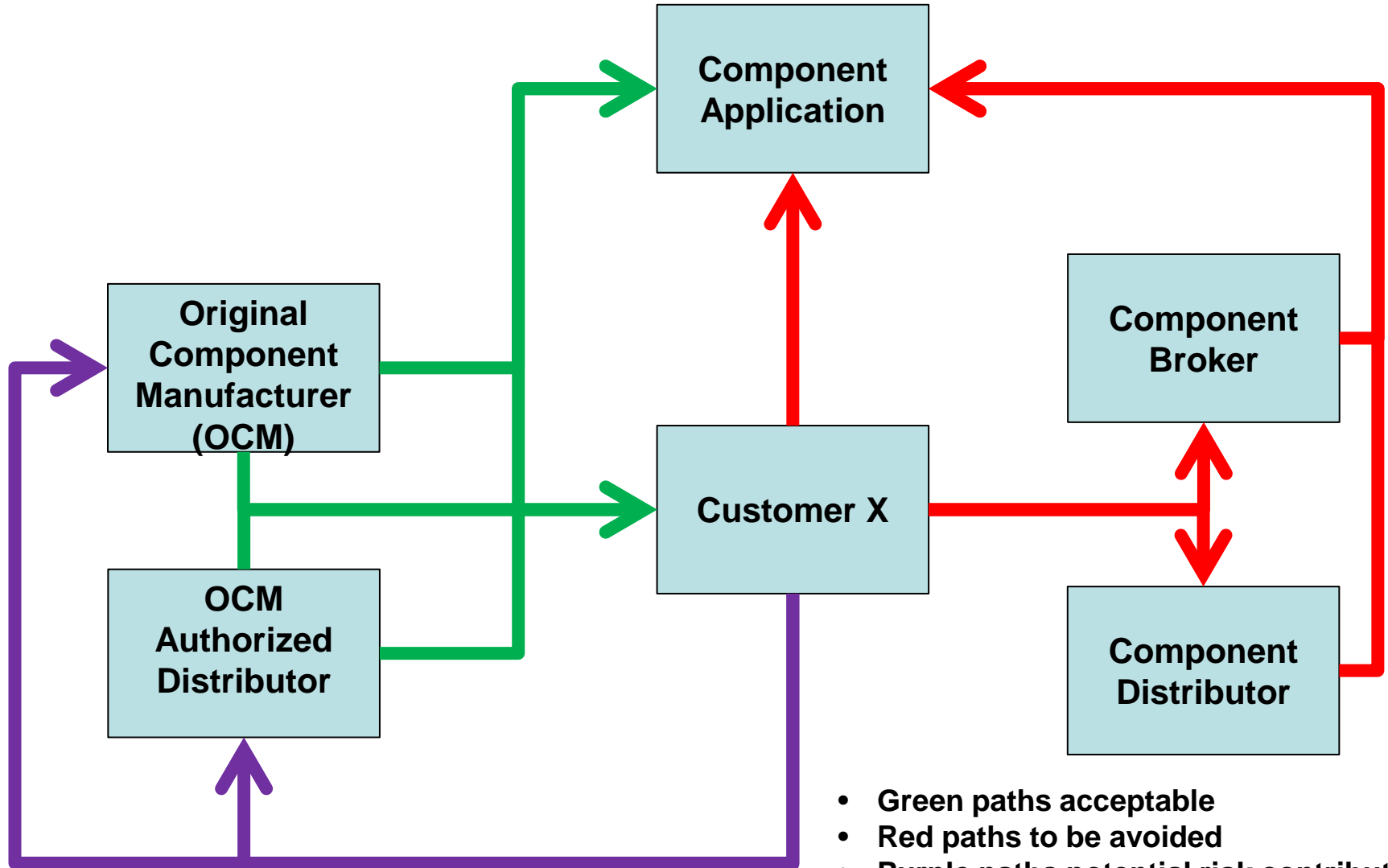
- **Top Counterfeit Sources\* Reported by OCMs**

- Brokers (50%)
- Non-Franchised Distributors (45%)
- Internet Exclusive Sources (36%)



**Counterfeit sources almost  
always outside the  
manufacturer's approved  
distribution channel**

\* U.S. Department of Commerce, Office of Technology Evaluation, Counterfeit Electronics Survey, November 2009



- Green paths acceptable
- Red paths to be avoided
- Purple paths potential risk contributor

- **18 U.S.C § 2320, codification of Trademark Counterfeiting Act, 1984, criminalizes counterfeiting**
- **FAR 52.203-13, Contractor Code of Business Ethics and Conduct**
  - Requires contractors to notify Inspector General and Contracting Officer of violations, including fraud
  - FAR 27.202-1 includes similar requirements
- **FAR 52.211-5, Material Requirements**
  - Prohibits use of used material without Contracting Officer approval
- **DODI 4140.67, DoD Counterfeit Prevention Policy**
  - Implements FY12 National Defense Authorization Act
  - Accompanying DFARS report due 25 Sep 2013 (Case 2012-D055)
- **Program Protection Plan (DODI 5200.39 and DODI 5000.02)**
- **Parts, Materials, and Processes contract statement of work inputs**
  - Requires Government approval for use of parts not from manufacturer approved distribution
  - Requires Government approval for parts with date codes over 5 years old

- Signed into law on 31 December 2011
- Includes a Federal Anti-Counterfeiting Amendment that requires development of DoD policies and regulations
  - Trusted suppliers must be used by DoD and DoD contractors
  - Requires all DoD contractors to report counterfeits and suspect counterfeits to GIDEP (or similar system defined by DoD); used parts represented as new to be covered by counterfeit definitions
  - Authorizes the **debarment of contractors who fail to detect and avoid counterfeit parts** or do not exercise adequate due diligence
  - Covered contractors\* are now **prohibited from charging the DoD for the costs of rework or corrective work** to remove and replace counterfeit parts
  - Covered contractors\* are **now responsible for the remedies required after the use or inclusion of counterfeit components** they may have accidentally supplied, regardless of where the counterfeit entered the supply chain

Requirements generally consistent with contract requirements suggested by AMRDEC for several years

\* Covers contractors for orders over \$5M, so small spares purchases may not be covered by these provisions



- **Require Government approved Parts Management Plans (per MIL-STD-3018) that include Counterfeit Risk Mitigation Plans (IAW SAE AS5553 and AS6174)**
- **Implemented contractual requirements since 2005 to exclude situations responsible for most counterfeit parts:**
  - **Parts not procured from the original manufacturer or a manufacturer certified distributor.**
  - **Reused, reinstalled, recycled, or salvaged parts or materials. Parts or materials previously installed or otherwise attached to another assembly are considered used and not new.**
  - **Parts with date codes more than 5 years old at the time of contract award without an approved recertification process**
- **Require Obsolescence Management Plans**



## **X.X Parts, Materials, and Processes (PMP) Plan**

**The contractor shall develop, implement, and maintain a PMP IAW DI-SDMP-81748, with government approval. The PMP Plan shall address the requirements of MIL-STD-3018, and .... In addition, the Plan shall include flow-down requirements for parts and materials, including off-the-shelf and non-developmental items, to suppliers for assemblies procured. The use of any of the problem PMPs listed in Attachment TBD#1 shall require government approval. The PMP program shall ensure that:**

- a. Parts performance ...**
- b. Materials utilized will ...**
- c. Processes utilized ...**
- d. Lead-free Control Plan. The Contractor shall prepare ... ,**
- e. Counterfeit Risk Management. The Contractor shall prepare, or update existing, Counterfeit Risk Management Plan for submittal and approval as a portion of the PMP Plan. The Plan shall meet the requirements of SAE AS5553 for electronics and SAE AS6174 for items not considered electronics. Components (or parts) not directly procured from the original component manufacturer (OCM) or the OCM's authorized distributor shall require Government approval. Contractors shall report counterfeits and suspected counterfeits to the Government and in the Government Industry Data Exchange Program.**
- f. Commercial Off-the-Shelf (COTS) Management. The Contractor shall prepare ...**

## **X.Y Obsolescence Management**

- **Verify inclusion/recognition of suitable regulations in contract**
  - **DFAR 252.246-7003, Notification of Potential Safety Issues**
  - **FAR 52.203-13, Contractor Code of Business Ethics and Conduct**
  - **FAR 52.211-5, Material Requirements**
- **Contractors need to provide Counterfeit Risk Management Plan, as portion of Parts, Materials, and Processes Management Plan**
  - **Government approval should be required to assure effectiveness**
  - **Intent of requirement must be met for all delivered hardware**
    - **Flow down requirement throughout supply chain**
    - **COTS requires special attention, as it must meet system requirements**
    - **In cases where COTS supplier is nonresponsive the contractor must take responsibility and have effective plan to manage risk**
- **Verify implementation of Program Protection Plan per OSD policy**
- **Report counterfeits and suspected counterfeits in GIDEP**

**Proper Definition and Implementation of Counterfeit Risk Mitigation Plan can meet the OSD policy IAW DODI 4140.67**

- **SAE AS5553 (electronics) and SAE AS6174 (non-electronics) requirements**
  - **Counterfeit control plan**
  - **Obsolescence management**
  - **Purchasing practices to preclude risk of counterfeits**
    - **Procure from original manufacturer (OCM) or their authorized suppliers**
    - **Establish approved suppliers when parts not available from OCM**
    - **Establish traceability to OCM**
    - **Utilize Excluded Parties List, and similar tools, to assess supplier risk**
      - <https://www.sam.gov/> (System for Award Management)
  - **Detection/Verification process**
    - **Apply methods to identify counterfeits depending on supply chain risk**
  - **Material control**
    - **Assure suspect parts do not reenter supply chain: quarantine**
  - **Reporting (GIDEP, ERAI, customer, etc.)**
    - **Verify FAR compliance to DODIG/contracting officer notification of counterfeits and suspect counterfeits, in addition to Program Office**

## **FY12 NDAA and OSD Policy has gotten attention! But ...**

- **Ineffective flow-down**
  - **Not taking responsibility for validating subcontractor plans**
    - **Not sufficient to just state in purchase orders that subs not deliver counterfeits**
- **Aversion to getting customer approval or even giving notification for non-preferred sources**
- **Stove-piped functions**
  - **Plans not enforcing coordination of key organizations, such as Purchasing, Quality, Component Engineering**
- **Reporting requirement not forceful or comprehensive**
  - **Commitment to GIDEP reporting still tepid**
  - **Plans typically don't require DOD IG and KO notification**
    - **Required by FAR, Business ethics on fraud reporting**