Counterfeit Part Awareness, Avoidance, & Risk Mitigation

George Young
April 2015
ASQLA
THIS PRESENTATION CONTAINS GENERAL, CONDENSED SUMMARIES OF ACTUAL REGULATORY OR RAYTHEON COMPANY REQUIREMENTS, OTHER COMPANY AND ORGANIZATIONS PRODUCTS OR SERVICES.

THE PRESENTATION IS FOR INFORMATION PURPOSES ONLY. IT IS NOT MEANT TO BE AND SHOULD NOT BE CONSTRUED AS LEGAL ADVICE OR ENDORSEMENT OF ANY SPECIFIC REGULATORY ITEM, PRODUCT OR SERVICE.
Counterfeit Avoidance & Risk Mitigation

- Definition(s)
- The Risk
- U.S. Regulatory Activity
- Counterfeit Risk Mitigation
- Supplier Engagement
- Standards & Resources
- Staying Informed
- Training Resources
- Emerging Detection
- Conclusion

Example of welded lead replacements
Counterfeit Definition(s)  SAE AS5553

3.1 Suspect Part
A part in which there is an indication that it may have been misrepresented by the supplier or manufacturer and may meet the definition of fraudulent part or counterfeit part provided below.

3.2 Fraudulent Part
Any suspect part misrepresented to the Customer as meeting the Customer’s requirements.

3.3 Counterfeit Part
A fraudulent part that has been confirmed to be a copy, imitation, or substitute that has been represented, identified, or marked as genuine, and/or altered by a source without legal right with intent to mislead, deceive, or defraud.

NOTE: The following diagram (Figure 2) depicts the above interrelationship between Suspect, Fraudulent and Counterfeit Parts. A Suspect Part may be determined to be, fraudulent or counterfeit through further evaluation and testing. All counterfeit parts are fraudulent, but not all fraudulent parts are counterfeit.

FIGURE 2 - INTERRELATIONSHIP BETWEEN SUSPECT, FRAUDULENT, AND COUNTERFEIT PARTS
“Counterfeit electronic part” means an unlawful or unauthorized reproduction, substitution, or alteration that has been knowingly mismarked, misidentified, or otherwise misrepresented to be an authentic, unmodified electronic part from the original manufacturer, or a source with the express written authority of the original manufacturer or current design activity, including an authorized aftermarket manufacturer. Unlawful or unauthorized substitution includes used electronic parts represented as new, or the false identification of grade, serial number, lot number, date code, or performance characteristics.

“Suspect counterfeit electronic part” means an electronic part for which credible evidence (including, but not limited to, visual inspection or testing) provides reasonable doubt that the electronic part is authentic.
Counterfeit Definition(s) Raytheon TC-001

Counterfeit Items include, but are not limited to, goods or separately-identifiable items or components of goods that:

(i) are an illegal or unauthorized copy or substitute of an OM item;

(ii) are not traceable to an OM sufficient to ensure authenticity in OM design and manufacture;

(iii) do not contain proper external or internal materials or components required by the OM or are not constructed in accordance with OM design;

(iv) have been re-worked, re-marked, re-labeled, repaired, refurbished, or otherwise modified from OM design but not disclosed as such or are represented as OM authentic or new; (v) have not passed successfully all OM required testing, verification, screening, and quality control processes; or

(vi) an item with altered or disguised documentation, package labeling, or item marking intended to mislead a person into believing a non-OM item is genuine, or that an item is of better or different performance when it is not.

Misrepresent & Intent / common theme across many definitions
Other Terms & Definitions

SAE AS5553

ELECTRICAL, ELECTRONIC, AND ELECTROMECHANICAL (EEE) PART:
Electrical, electronic, and electromechanical parts are components designed and built to perform specific functions, and are not subject to disassembly without destruction or impairment of design use. Examples of electrical parts include resistors, capacitors, inductors, transformers, and connectors. Electronic parts include active devices, such as monolithic microcircuits, hybrid microcircuits, diodes, and transistors. Electromechanical parts are devices that have electrical inputs with mechanical outputs, or mechanical inputs with electrical outputs, or combinations of each. Examples of electromechanical parts are motors, synchros, servos, and some relays.

DFARS 252.246-7007

“Electronic part” means an integrated circuit, a discrete electronic component (including, but not limited to, a transistor, capacitor, resistor, or diode), or a circuit assembly (section 818(f)(2) of Pub. L. 112-81). The term “electronic part” includes any embedded software or firmware.
Other Terms & Definitions

SAE AS5553

BROKER:
In the independent distribution market, Brokers are professionally referred to as Independent Distributors. See definitions for “Broker Distributor” and “Independent Distributor.”

INDEPENDENT DISTRIBUTOR:
A distributor that purchases parts with the intention to sell and redistribute them back into the market. Purchased parts may be obtained from Original Equipment Manufacturers (OEMs) or Contract Manufacturers (typically from excess inventories), or from other Distributors (Franchised, Authorized, or Independent). Resale of the purchased parts (redistribution) may be to OEMs, Contract Manufacturers, or other Distributors. Independent Distributors do not normally have contractual agreements or obligations with OCMs. See definition of “Authorized (Franchised) Distributor.”

DFARS 252.246-7007
No definition provided
Other Terms & Definitions

SAE AS5553

AUTHORIZED (FRANCHISED) DISTRIBUTOR:
Distributor when they perform Authorized Distribution.

AUTHORIZED DISTRIBUTION:
Transactions conducted by an OCM-Authorized Distributor distributing product within the terms of an OCM contractual agreement. Contractual Agreement terms include, but are not limited to, distribution region, distribution products or lines, and warranty flow down from the OCM. Under this distribution, the distributor would be known as an Authorized Distributor. For the purposes in this Standard, Franchised Distribution is considered synonymous with Authorized Distribution.

DFARS 252.246-7007
No definition provided however System Criteria (5) provides the following (5) Use of suppliers that are the original manufacturer, or sources with the express written authority of the original manufacturer or current design activity, including an authorized aftermarket manufacturer or suppliers that obtain parts exclusively from one or more of these sources…
Counterfeit Avoidance & Risk Mitigation

- Definition(s)
- The Risk
- U.S. Regulatory Activity
- Counterfeit Risk Mitigation
- Supplier Engagement
- Standards & Resources
- Staying Informed
- Training Resources
- Emerging Detection
- Conclusion

Example of welded lead replacements
Overview of Counterfeit Parts

- Counterfeiting affects all industries; electronics is a focus
- E-waste is a main source of supply
- Obsolescence provides a source of demand
- Distributed mainly through non-franchised distributors
- Increasing incident volume and variety
- Counterfeiting is price independent

Counterfeits impact all industries
Counterfeit Risk

- **68 GIDEP Alerts in 2014**
  - Majority are for electronic components
  - Two alerts since 2013 involve authorized distribution
  - Non electronic component items: network switches, hard drives, UL / Test Lab marks, tape

- **Over 700 Suspect Counterfeit Reports in ERAI Alerts During the Past 12 Months**

Persistent Risk Requires Robust Processes

http://www.erai.com/ca_Counterfeit_Awareness

ERAI image used by permission of ERAI. GIDEP logo and images used by permission of GIDEP
Counterfeit Risk

Electronics is Primary Risk but not the only Risk

DLA Federal Supply Group Focus
- FSG 59 (Electrical and Electronic Equipment Components)
- FSG 29 (Engine Accessories)
- FSG 47 (Pipe, Tubing, Hose, and Fittings)
- FSG 53 (Hardware & Abrasives)
- FSG 25 (Vehicular Equipment Components)
- FSG 31 (Bearings)

ERAI 6200 +
GIDEP 600 +
Trend

ESCO Anti-Countering Forum
Suspected Device Detail Reports

ERAI image used by permission of ERAI, GIDEP images used by permission of GIDEP, eTCP-SAS-5942
Counterfeiting “Raw Materials”

Washing components in river

Components on river bank drying
Part Removal & Storage

0402 Case Size Capacitors
($0.005 ea from Fran. Disty)
Counterfeit Examples

14V 0.5W Zener Diode
- Smaller die
- No / poor metallurgical bond
- Smaller package with pure tin terminations vs OEM tin / lead termination
- OEM stated parts were not manufactured by them. Smaller die size indicative of commercial part produced by another manufacturer.

SLOPPY BLACK-TOPPING

Authentic                  Counterfeit

SMT photographs used by permission of SMT Corporation
Additional Counterfeit Examples

Counterfeit factory box

Criminal Intelligence Bulletin
2007-001

Counterfeit CISCO Products

The purpose of this Criminal Intelligence Bulletin is to alert the Law Enforcement (LE) community to the threat posed by imitation CISCO products used in DoD systems.

At least five DCIS investigations have uncovered counterfeit CISCO routers, network cards, and switches being supplied to DoD, including Army, Navy, and Air Force. Several DoD entities (listed below) have procured counterfeit CISCO products and deployed them throughout the Global Information Grid. Using counterfeit products is significant because the items are not made with the same level of quality control as the authentic product and are often found to have improper shielding, which can lead to radiation exposure and fire hazards. Imitation parts also have a higher failure rate than their authentic versions, and are neither a designated nor authorized item in any DoD procurement contract.

There is also the possibility that these products could perform malicious network act...
Remarking example

CCA failure analysis
CCA produced by contract manufacturer.
Component manufacturer identified on the part confirmed they did not produce parts with this date code.
Remarking via Laser, also evidence of a cover coat. Multiple die configurations found.
Counterfeit Avoidance & Risk Mitigation

- Definition(s)
- The Risk
- U.S. Regulatory Activity
- Counterfeit Risk Mitigation
- Supplier Engagement
- Standards & Resources
- Staying Informed
- Training Resources
- Emerging Detection
- Conclusion

Example of welded lead replacements
### US Government & Standards Activity

<table>
<thead>
<tr>
<th>Date</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oct 2008</td>
<td>Business Week Article</td>
</tr>
<tr>
<td>Dec 2008</td>
<td>US DoC Survey Published</td>
</tr>
<tr>
<td>Apr 2009</td>
<td>AS5553 Published Jan 2013 Rev A</td>
</tr>
<tr>
<td>Oct 2010</td>
<td>US DoC Survey Collection</td>
</tr>
<tr>
<td>Jan 2010</td>
<td>US SASC Review Begins</td>
</tr>
<tr>
<td>Feb 2011</td>
<td>US SASC Hearings</td>
</tr>
<tr>
<td>Nov 2011</td>
<td>HR1540 Becomes Law</td>
</tr>
<tr>
<td>Dec 2011</td>
<td>ARP6178 Published</td>
</tr>
<tr>
<td>Mar 2012</td>
<td>Frank Kendall Memo</td>
</tr>
<tr>
<td>Mar 2012</td>
<td>DCMA Assessment tasking</td>
</tr>
<tr>
<td>Feb 2012</td>
<td>US GAO Report on Internet</td>
</tr>
<tr>
<td>Mar 2012</td>
<td>DLA QTSL</td>
</tr>
<tr>
<td>Aug 2012</td>
<td>DFAR 2012-D055 Opens</td>
</tr>
<tr>
<td>Nov 2012</td>
<td>AS6081 Published</td>
</tr>
<tr>
<td>Apr 2009</td>
<td>AS5553 (DoD Adopted)</td>
</tr>
<tr>
<td>SAE AS6081</td>
<td>Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition - Distributors</td>
</tr>
<tr>
<td>SAE AS6171</td>
<td>Test Methods Standard; Counterfeit Electronic Parts</td>
</tr>
<tr>
<td>SAE AS6174</td>
<td>Counterfeit Material; Assuring Acquisition of Authentic and Conforming Material</td>
</tr>
<tr>
<td>SAE ARP6178</td>
<td>Fraudulent/Counterfeit Electronic Parts; Tool for Risk Assessment of Distributors - Includes Access to Additional Content</td>
</tr>
</tbody>
</table>

#### Build up to US Procurement Regulations

- SAE AS5553A: Fraudulent/Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition (DoD Adopted)
- SAE AS6081: Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition - Distributors
- SAE AS6171: Test Methods Standard; Counterfeit Electronic Parts
- SAE AS6174: Counterfeit Material; Assuring Acquisition of Authentic and Conforming Material
- SAE ARP6178: Fraudulent/Counterfeit Electronic Parts; Tool for Risk Assessment of Distributors - Includes Access to Additional Content

**Timeline:**
- **Dec 2008**: US DoC Survey Published
- **Jan 2010**: US SASC Review Begins
- **Feb 2011**: US SASC Hearings
- **Nov 2011**: HR1540 Becomes Law
- **Dec 2011**: ARP6178 Published

**Key Dates:**
- **Oct 2008**: Business Week Article
- **Dec 2008**: US DoC Survey Published
- **Jan 2009**: AS5553 Published Jan 2013 Rev A
- **Oct 2010**: US DoC Survey Collection
- **Jan 2010**: US SASC Review Begins
- **Feb 2011**: US SASC Hearings
- **Nov 2011**: HR1540 Becomes Law
- **Dec 2011**: ARP6178 Published
- **Jan 2012**: Frank Kendall Memo
- **Mar 2012**: DCMA Assessment tasking
- **Feb 2012**: US GAO Report on e-Waste
- **Feb 2012**: US GAO Report on Internet
- **Mar 2012**: DLA QTSL
- **Aug 2012**: DFAR 2012-D055 Opens
- **Nov 2012**: AS6081 Published
US Regulatory Activity

2012 National Defense Authorization Act Section 818

2014 National Defense Authorization Act, Section 803

2015 National Defense Authorization Act Section 817

DFARS 252.246-7007 Released

2013 National Defense Authorization Act Section 833

2014 National Defense Authorization Act, Section 803

Open DFARS Cases
Open FAR Cases

2015 National Defense Authorization Act Section 817

2013 DoD Instruction 4140.67

Regulatory Requirements In Development
DFARS/FAR Cases of Interest

DFARS Case 2012-D055: Detection and Avoidance of Counterfeit Parts
- Counterfeit avoidance becomes part of contractor purchasing system

DFARS Case 2014-D005: Detection and Avoidance of Counterfeit Electronic Parts – Further Implementation
- Anticipated regulations for smaller businesses and non CAS covered contractors

FAR Case 2012-032: Higher Level Contract Quality Requirements
- Revised the Quality Management flow down environment

FAR Case 2013-002: Expanded Reporting of Nonconforming Supplies
- May significantly increase reporting requirements for non-conforming material
DFARS 252.246-7007 Summary

- DFARS 252.246-7007 for Counterfeits released 05/06/14
- Partial implementation of 2012 & 2013 NDAA requirements
- Effective 05/06/14
- First of four planned regulations (DFARS and FARs)
- “risk based provides for flexibility on how contractors interpret and implement the 12 system criteria.
- Government Agencies (DCMA, DPAP, etc.) have not yet given further definitive guidance on what will be acceptable.
1) The training of personnel.

2) The inspection and testing of electronic parts, including criteria for acceptance and rejection.

3) Processes to abolish counterfeit parts proliferation.

4) Processes for maintaining electronic part traceability (e.g., item unique identification) that enable tracking of the supply chain back to the original manufacturer, whether the electronic parts are supplied as discrete electronic parts or are contained in assemblies....

5) Use of suppliers that are the original manufacturer, or sources with the express written authority of the original manufacturer or current design activity, including an authorized aftermarket manufacturer or suppliers that obtain parts exclusively from one or more of these sources. When parts are not available from any of these sources, use of suppliers that meet applicable counterfeit detection and avoidance system criteria.

6) Reporting and quarantining of counterfeit electronic parts and suspect counterfeit electronic parts. Reporting is required to the Contracting Officer and to the Government-Industry Data Exchange Program (GIDEP) when the Contractor becomes aware of....

7) Methodologies to identify suspect counterfeit parts and to rapidly determine if a suspect counterfeit part is, in fact, counterfeit.
8) Design, operation, and maintenance of systems to detect and avoid counterfeit electronic parts and suspect counterfeit electronic parts. The Contractor may elect to use current Government- or industry-recognized standards to meet this requirement.

9) Flow down of counterfeit detection and avoidance requirements, including applicable system criteria provided herein, to subcontractors at all levels in the supply chain that are responsible for buying or selling electronic parts or assemblies containing electronic parts, or for performing authentication testing.

10) Process for keeping continually informed of current counterfeiting information and trends, including detection and avoidance techniques contained in appropriate industry standards, and using such information and techniques for continuously upgrading internal processes.

11) Process for screening GIDEP reports and other credible sources of counterfeiting information to avoid the purchase or use of counterfeit electronic parts.

12) Control of obsolete electronic parts in order to maximize the availability and use of authentic, originally designed, and qualified electronic parts throughout the product’s life cycle.
Challenges

• Electronic Part includes embedded software and firmware
• Unallowable costs, with little opportunity to make allowable
• Counterfeit detection and avoidance systems now in CPSR
• Commercial items and COTS are in scope
• Traceability in supplier base of piece part and parts in assemblies
• No grandfather clause for inventory in supply base
• GIDEP reporting and screening within global supply base
• Impact to small businesses
Counterfeit Avoidance & Risk Mitigation

- Definition(s)
- The Risk
- U.S. Regulatory Activity
- Counterfeit Risk Mitigation
- Supplier Engagement
- Standards & Resources
- Staying Informed
- Training Resources
- Emerging Detection
- Conclusion

Example of welded lead replacements
Raytheon Company Approach

- Raytheon utilizes a standardized, risk based approach
- Prevention focus: electronics, materials, mechanical, assemblies and test equipment
- Obsolescence management is key
- OEM preferred; Five brokers with testing
- Supply Base:
  - Optimization
  - Awareness
  - Requirement Flow Down
  - Assessment
- GIDEP reporting on all incidents
- Suspect material does not return to Supply Chain

Lower Risk through Robust Process and Tools
Raytheon Company Approach

Example of Raytheon Counterfeit Risk Mitigation Requirement

- Identifies specific tests & inspection
- Defines sample requirements
- Requires data review by Raytheon

<table>
<thead>
<tr>
<th>Inspection/Test</th>
<th>Requirement</th>
<th>Sample Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packaging Inspection and OEM/OCM history Investigation</td>
<td>Verification that package marking is consistent with the OEM marking and that the date / lot code is not later than the last production date. For Qualified Parts List (QPL) parts, verify that the manufacturer identified on the package was a QPL source for the time period represented by the part date / lot code.</td>
<td>3 parts from each date code</td>
</tr>
<tr>
<td>External Visual Inspection</td>
<td>IDEA-STD-1010, 20 X magnification minimum, 50 X or greater may be used to detect counterfeiting</td>
<td>100% up to 45 pieces and minimum 45 piece sample for lots greater than 45 pieces</td>
</tr>
<tr>
<td>Mechanical Inspection</td>
<td>IDEA-STD-1010 paragraph 10.3.3</td>
<td>20 parts from each date code</td>
</tr>
<tr>
<td>Marking Permanency</td>
<td>Using the following in the order specified: 1) 3 parts Mineral Spirits, 1 part Isopropyl Alcohol mixture, 2) Acetone</td>
<td>3 parts from each date code</td>
</tr>
<tr>
<td>Backtop Testing</td>
<td>1) 1-Methyl 2- Pyrrolidone (AS6081), 2) Dynasolve 750 solution (AS6081), 3) Scrape Test (IDEA 1010.3.2.3)</td>
<td>3 parts from each date code</td>
</tr>
<tr>
<td>Delid / Decapsulation</td>
<td>Component Decap (cavity devices only) and die photograph to compare die marking to external part marking, OEM/OCM die maps or datasheet or known good die, if available</td>
<td>3 parts from each date code</td>
</tr>
<tr>
<td>Lead Cross-Section</td>
<td>For metal can, through hole packages such as TO-99, TO-100, TO-8, etc. All device leads must be cross-sectioned in order to determine if leads have been extended by welding</td>
<td>3 parts from each date code, all leads (may be performed on the Delid / Decapsulation sample)</td>
</tr>
<tr>
<td>Solderability</td>
<td>per IPC/EIA-J-STD-002</td>
<td>3 parts from each date code</td>
</tr>
<tr>
<td>X-Ray Fluorescence</td>
<td>Termination finish composition</td>
<td>3 parts from each date code</td>
</tr>
<tr>
<td>Electrical</td>
<td>Test in accordance with commodity matrix in Appendix A herein</td>
<td>100%</td>
</tr>
<tr>
<td>Radiographic Inspection</td>
<td>Radiographic Inspection of the die and internal construction of the product</td>
<td>100%</td>
</tr>
</tbody>
</table>
Raytheon Approach

Organizational Resources
Tools, Training, Communication

COUNTERFEIT MATERIAL AVOIDANCE

<table>
<thead>
<tr>
<th>OVERALL RESULTS OF PPV FOR THIS PROCESS</th>
<th>DETAILS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is process in control and effective?</td>
<td></td>
</tr>
<tr>
<td>If there is a contractual flowdown, is the supplier meeting that requirement?</td>
<td></td>
</tr>
<tr>
<td>Has Raytheon identified this as a key process as relates to KFC Management?</td>
<td></td>
</tr>
<tr>
<td>If there is controlled documentation that outlines elements of this process, is it readily available?</td>
<td></td>
</tr>
<tr>
<td>Is there a method the supplier uses to monitor effectiveness of process?</td>
<td></td>
</tr>
<tr>
<td>Was hardware reviewed?</td>
<td></td>
</tr>
<tr>
<td>Was hardware reviewed acceptable?</td>
<td></td>
</tr>
<tr>
<td>Were the supplier’s inspection documentation reviewed in preparation for this PPV?</td>
<td></td>
</tr>
</tbody>
</table>

EVALUATION AREAS

1.1 PROCUREMENT POLICY AND PROCEDURES
   - Is the company’s采购 policy and procedures being followed? How? Why? Are they documented on an Action Status Tab?

LESSONS LEARNED!

Materials & Mechanical

Enterprise Resources
Raytheon Requirement Documents

Counterfeit Specific Quality Notes

GP: Counterfeit Electronic Part Risk Mitigation
WE: Counterfeit Material Avoidance Process Requirements
WK: Metal Procurement Certification and Traceability Requirements
WL: Counterfeit Risk Mitigation, Chemical, Gas, Non-Metallic, Raw Material
WM: Counterfeit Risk Mitigation, Mechanical Part
WN: Counterfeit Risk Mitigation, Fab, Molded, Plastic and Rubber Parts

www.raytheon.com/connections/supplier/index.html
Key Counterfeit Avoidance Requirements

- **TC-001 General Terms and Conditions of Purchase (04/13)**
  13(b)
  - Goods are and only contain material from OM or OM Authorized source
  - Not be or contain Counterfeit items
  - Definition for Counterfeit Goods
  - DFARS 252.246-7007

- **TC-004 International General Terms and Conditions of Purchase (04/13)**
  13(b)
  - Goods are and only contain material from OM or OM Authorized source
  - Not be or contain Counterfeit items
  - Definition for Counterfeit Goods
  - DFARS 252.246-7007

- **TC Hardcode (12/13) (10)**
  - Notification and authorization if materials cannot be obtained from OM or OM Authorized Source
  - Flow down of counterfeit risk mitigation requirement to sub tiers

- **TC013 (12/11) Warranty For Goods Obtained From Brokers**
  - When used replaces Section 13 of TC-001 or TC-004

- **Quality Note WE**
  - Counterfeit Risk Mitigation using SAE AS5553 as a guide. (supplier & supplier sub tiers)
  - GIDEP participation monitor & acting on alerts
  - Communication details if procurement from other than OM or OM Authorized Source is required
  - Flow down of requirements

Ensure Requirements are Understood & Definitions Align
Counterfeit Avoidance & Risk Mitigation

- Definition(s)
- The Risk
- U.S. Regulatory Activity
- Counterfeit Risk Mitigation
- Supplier Engagement
- Standards & Resources
- Staying Informed
- Training Resources
- Emerging Detection
- Conclusion

Example of welded lead replacements
Raytheon Expectations

- Establish a counterfeit prevention, detection and risk mitigation policy aligned with Industry and DoD requirements
- Robust, active obsolescence management
- Procure from OEM/OCM or their authorized resellers
- Use non-OEM/authorized sources ONLY for obsolete items
- Implement training and maintain counterfeit avoidance and detection competencies
- Robust supplier assessment and minimum quantity of independent distributors
- Specify and confirm counterfeit detection test and analysis requirements
- Monitor and report to GIDEP or regional equivalent
- Keep suspect counterfeit material out of the Supply Chain
- Measure, communicate and report
- Accept and meet DFARS 252.246-7007

Preferred Sources, Robust Counterfeit Prevention
Raytheon Enterprise Supplier Assessment (RESA)

1. Enterprise process for assessing supplier capabilities, promoting educated and informed decisions.
2. Assessments are a collaboration of Raytheon Supply Chain, Mission Assurance, Program Management and Engineering, along with our valued suppliers in an effort to mitigate risk and maximize performance.

Includes Eight Assessment Checklists

RESA Process and Tools
- Chapter 0: Quality Management Systems Audit
- Chapter 1: New Supplier Capability Assessment
- Chapter 2: Existing Supplier Capability Assessment
- Chapter 3: Supplier Total Business Assessment
- Chapter 4: Pre-work Authorization Review
- Chapter 5: Post-award Review
- Chapter 6: Periodic Total Business Assessment
- Chapter 7: Product and Process Verification
- Chapter 8: Counterfeit Avoidance & Risk Mitigation

Chapter 8, Counterfeit Avoidance & Risk Mitigation Focuses on:
- Industry Standards
- Raytheon & Regulatory Requirements
- Lessons Learned
Lessons Learned from Recent RESA Engagements

- OM / authorized sources
- Customer notification
- Awareness, training and expertise
- Due diligence
- Industry alerts
- Sub tier supplier assessment

Process Details and Sub Tier Assessment Are Key
Supplier Assessment Resources

- SAE ARP 6178 Fraudulent/Counterfeit Electronic Parts; Tool for Risk Assessment of Distributors (2011)
  - Pre Assessment Information
  - Quality System and Processes
  - Supplier Qualification & Purchasing Process
  - Training & Certifications
  - Nonconforming Material
  - 160 Questions
  - Recommended Rating Criteria & MS Excel template allows for custom weighting

  - General Information
  - Parts Inspection, Verification & Handling
  - Nonconforming Material
  - Document Control & Record Retention
  - Liability & Disposition
  - 67 Questions
  - Guidance provided for each question
  - Procurement
  - Training
  - Corrective Action
  - Reporting of Suspect Parts
Counterfeit Avoidance & Risk Mitigation

- Definition(s)
- The Risk
- U.S. Regulatory Activity
- Counterfeit Risk Mitigation
- Supplier Engagement
- Standards & Resources
- Staying Informed
- Training Resources
- Emerging Detection
- Conclusion

Example of welded lead replacements
## SAE Standards Activity

### SAE G-19 & G-21 Committee Products

<table>
<thead>
<tr>
<th>G-19 Counterfeit Electronic Components Committee</th>
<th>G-21 Counterfeit Materiel Committee</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Profiler Test Provider</strong>&lt;br&gt; (ISO/IEC 17025 Accredited)</td>
<td><strong>Certification Body</strong>&lt;br&gt; (IAF &amp; ISO/IEC 17021 Accredited)</td>
</tr>
<tr>
<td>Operator(s) Certified to PT Scheme for identified AS6171 Test Scheme</td>
<td></td>
</tr>
<tr>
<td><strong>Test Provider</strong>&lt;br&gt; (Accredited to ISO/IEC 17025 &amp; Certified to AS9100 and/or ISO 9001)</td>
<td><strong>Test Provider</strong>&lt;br&gt; (Certified to AS9100 and/or ISO 9001)</td>
</tr>
<tr>
<td><strong>Original Component Manufacturer</strong>&lt;br&gt; (Certified to AS9100 and/or ISO 9001)</td>
<td><strong>Distributor</strong>&lt;br&gt; (Certified to AS9120 and/or ISO 9001)</td>
</tr>
<tr>
<td><strong>Authorized/ Franchised</strong></td>
<td><strong>Broker/ Independent</strong></td>
</tr>
</tbody>
</table>

### SAE Products

- **AS6171**, Test Methods Standard; Counterfeit Electronic Parts Document in progress. SAE G-19A
- **ASxxxx**, OCM Counterfeit Mitigation Subcommittee. Subcommittee Proposed. SIA, SRC Proposed Co-Chairpeople, SAE G-19O
- **AS6496**, Authorized Distributor Counterfeit Mitigation Published August 2014 SAE G-19AD
- **ARP6178**, Counterfeit Electronic Parts; Tool for Risk Assessment of Distributors. Worksheet and User Guide Published December 2011 SAE G-19DR
- **AS6462**, AS5553, Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition Verification Criteria Includes Audit Checklist. Published November 2012 Rev. A Published August 2014 SAE G-19C
- **AS6886**, Counterfeit Materiel; Assuring Acquisition of Authentic and Conforming Materiel Published August 2014 SAE G-21

### SIA Standards

- **AIR6273**, Terms and Definitions – Fraudulent/Counterfeit Electronic Parts. Document in progress. SAE G-19T

### Possible Future Work

- **ASxxxx**, Compliance Standard or Guide (Includes Audit Checklist) SAE G-19C
- **ASxxxx**, Compliance Standard or Guide (Includes Audit Checklist) SAE G-19C
- **ASxxxx**, Compliance Standard or Guide (Includes Audit Checklist) SAE G-19C

### Additional Information

- **ASxxxx**, Anti-Tamper and Transportation Security Subcommittee Proposed. TAPA, CBP, Express Carrier Proposed Co-Chair people, G-19AT

---

**4/8/2015** 39
UK Activity & Resources

Electronic Systems Community (ESCO) Anti-Counterfeiting Forum

- Potential Solution Providers
- Best Practices
- Suspect / Alleged Counterfeits
- Other Resources
- Push Mail

www.anticounterfeitingforum.org.uk
Additional Standards, Handbooks and Reports

- Electronics & Electromechanical
- Risk Assignment & Mitigation
- Test & Analysis, Photos
  https://standards.nasa.gov/documents/detail/3315823

Electric Power Research Institute (EPRI) (2014)
  Counterfeit and Fraudulent Items-Mitigating the Increasing Risk
- Power Generation Perspective
- Non Electronics Examples
  www.epri.com/abstracts/Pages/ProductAbstract.aspx?
  ProductId=000000000001019163

Aerospace Industry Association Special Report (2011)
- Aerospace & Defense Focus

- Space & Defense Aerospace Focus
  library.mailbox@aero.org
Web Resources

SAE Aerospace
Counterfeit Parts Portal

counterfeitparts.sae.org

International Aerospace Quality Group
Supply Chain Management Handbook (SCMH)
April 2014

- Industry Overview
- Definitions
- Risk Mitigation Strategies
- Key Control Processes for Mitigating Risk
- Training
- Obsolescence
- Procurement
- Product Verification
- Investigations
- Reporting

www.iaqg.org.scmh
Authorized Distributor Identification Resources

Web Services

http://www.eciaauthorized.com/

Subscription Services


http://www.siliconexpert.com/

Images used by permission of ECIA, Source ESB, IHS, Siliconexpert Technologies

Counterfeit Risk Analysis
Counterfeit Avoidance & Risk Mitigation

- Definition(s)
- The Risk
- U.S. Regulatory Activity
- Counterfeit Risk Mitigation
- Supplier Engagement
- Standards & Resources
- Staying Informed
- Training Resources
- Emerging Detection
- Conclusion

Example of welded lead replacements
Workshops and Symposiums

Conference 2015 Event Overview

ERAI Executive Conference 2015
- Register Now
- Event Overview
- Conference Schedule
- Speakers & Instructors
- Downloads
- Corporate Sponsors
- Exhibitors
- Testimonials
- Hotel/Travel
- Abstracts
- Sponsorship Opportunities
- Exhibitor Opportunities

2015 ERAI Executive Conference - Event Overview

SUPPLY CHAIN SECURITY: A MOVING TARGET
Succeeding in the Age of Counterfeits, Cyber Attacks, Seized Shipments & Diminishing Resources

APRIL 22-23, 2015
ERAI Executive Conference
Bayfront Hilton, San Diego, CA

The ERAI Executive Conference is the premier gathering for individuals and organizations involved in the purchase, sale or use of electronic parts and/or assemblies.

Product seizures, tight budgets, reporting and other contractual obligations imposed by new and impending regulations have organizations of all types scrambling to meet ever-expanding customer expectations. Using this year’s theme, “Supply Chain Security: A Moving Target,” as our backdrop, ERAI has set the stage to cumulatively measure our industry’s progress in the fight against counterfeit electronic parts while taking a deeper dive into the lesser-traveled territory of cyber attacks, talk of eliminating all surplus inventories from the open market and other security vulnerabilities.

Click here to download the 2015 ERAI Executive Conference Brochure

How do you hit a moving target?
Supply chain security is not static. It is a constantly moving and evolving target. To hit a moving target, you don’t aim at where it is now; you...
Workshops and Symposia

Symposium on Counterfeit Parts and Materials
June 23-25, 2015
College Park Marriott Hotel and Conference Center
College Park, MD

Technical Symposiums: June 23-25, 2015
Workshops: June 23, 2015
 Expo: June 23-24, 2015
University of Maryland, College Park, MD

SMTA and CALCE @ University of Maryland are pleased to announce the east coast venue for the Symposium on Counterfeit Parts and Materials. The program will be held June 23-25 at the Marriott Inn & Conference Center next to the University of Maryland. Don’t miss this opportunity to learn from and share your insights with government, industry and academics who are addressing the counterfeit problem.

Changes in electronic supply chain had been fast and furious in the last decades and its impact on the practices of companies is still evolving. It is well understood that, the occurrence of counterfeit electronic parts is related to the changes in supply chain but it is only one of the many impacts. This symposium will provide a forum to cover all aspects of changes in the electronic parts supply chain on how an organization performs part selection and management through whole life cycle of the part.

Using beyond anecdotes and examples of counterfeit parts, this symposium focuses on the solutions that are available and are under development by all sectors of the industry.

Topics will include:
• impact of supply chain changes on the component management practices: quality, reliability, manufacturability
• Electronic parts distribution: current stage and evolution
• Authentication techniques for securing electronic part supply chain
• Federal procurement practices and its impact on electronic supply chain
• Innovations tools and techniques for detecting counterfeit parts
• New areas of counterfeit concerns: materials, energy storage
• Industry and international working groups and standards on electronic part supply chain and counterfeit electronic parts

The symposium is organized by SMTA in conjunction with Center for Advanced Life Cycle Engineering (CALCE) at the University of Maryland, College Park, MD, USA. This symposium will be valuable to quality and reliability manager, supply chain manager, brand protection specialists, inspectors, marketing and procurement policy makers, contracts and legal management, security specialists and government agencies. Our focus is to provide relevant information to the professionals that can be used for solving problems today while planning for a different business and technology environment in the future.

www.smta.org/counterfeit

SMTA Image used by permission of SMTA. DMSMS image provided as media ad on the DMSMS web site.

Raytheon
Counterfeit Avoidance & Risk Mitigation

- Definition(s)
- The Risk
- U.S. Regulatory Activity
- Counterfeit Risk Mitigation
- Supplier Engagement
- Standards & Resources
- Staying Informed
- Training Resources
- Emerging Detection
- Conclusion

Example of welded lead replacements
Training Resources

• Counterfeit Products Overview
  • Available on Raytheon Web Site under Supplier Connections

• Course Objectives
  • Define counterfeit products and describe why they are a threat to Raytheon and our end users.
  • List the most common ways counterfeit products are introduced into the product’s lifecycle.
  • Identify the proper mitigation strategies to reduce risks associated with counterfeit parts
  • Define the roles and responsibilities associated with counterfeit risk mitigation and prevention.

Overview and Awareness Training

• http://www.raytheon.com/media/modules/corpcou0012/sclist.htm
Training Resources

- Defense Acquisition University
  - CLL 032 Preventing Counterfeit Electronic Parts from Entering the DoD Supply System (March 2014)
    - Types of Non Conforming & Suspect Counterfeit Items
    - How Counterfeits enter the supply chain
    - Economic Impact
    - Skills for identifying Counterfeits
    - Risk mitigation
    - Reporting
  
  - CLL 062 Counterfeit Prevention Awareness (March 2014)
    - Issues of Counterfeit Material
    - Impact on DoD programs
    - Means to Identify Counterfeits
    - Reporting and Disposition
Training Resources

- Counterfeit Products Overview
  - Materials available on NASA JPL Web Site
  - Three Courses
    - Counterfeit Parts Awareness Basic
    - Counterfeit Parts Awareness Intermediate
    - Counterfeit Parts Inspection Training

Counterfeit Parts Awareness - Basic
Description:
The spread of counterfeit electronic components continues to grow within the global supply chain and has penetrated various governmental agencies, including NASA and the US Department of Defense. The risk of counterfeit electronics being used in military equipment prompted an authorization act by Congress. The Authorization Act mandates NASA to develop and implement guidelines, detect, track, and catalog and reduce the number of counterfeits in the NASA supply chain.

This is an introductory awareness class. Objectives include:
- gain a basic understanding of the electronics supply chain
- gain basic knowledge of the supply chain
- gain familiarity with some of the methods
- examine risk mitigation steps
- Review verification and inspection processes

Prerequisite: None
Length: Approximately 4 hours

Counterfeit Parts Awareness - Intermediate
Description:
This is a follow-on course to the Basic. Objectives include:
- Explore concepts regarding inspection (concepts introduced in Basic)
- Present guidance for supply chain
- Examine the concept of parts risk
- Overview of pertinent unit

Prerequisite: Counterfeit Parts Awareness Basic
Length: Approximately 4 hours

Counterfeit Parts Inspection Training
Description:
This is a follow up class to the JPL Counterfeit Parts Awareness Class. Objectives include:
- Gain in-depth knowledge of inspection tools and equipment used for part authentication
- Gain hands-on experience inspecting actual electronic components

Prerequisite: Counterfeit Parts Awareness - Basic
Length: approximately 4 hours

Images used in accordance with JPL Image Use Policy.
http://mttc.jpl.nasa.gov/
Training Resources

- Counterfeit Parts Definitions & Origins
- MDA Documents & Supplier Definitions
- MDA Experience with Counterfeits
- DoD Requirements

Training Objectives

- Become aware of the counterfeit parts risk.
- Learn about MDA requirements, and the impact of counterfeit parts to MDA.
- Understand the mission impact from counterfeit parts or equipment.
- Realize the need for rigorous parts control and procurement vigilance against these threats.
- Learn about counterfeit part types, and how to detect and report them.
- Learn what MDA and the Department of Defense (DoD) are doing about the problem.

Note: This document contains both DoD-specific and commercial data.

MDA COUNTERFEIT PART TRAINING

AVOIDANCE, DETECTION, CONTAINMENT, AND REPORTING

Approved for Public Release
13-MDA-7946 (11 December 13)
DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited.
December 11, 2013

- MDA Requirements & Recommendations
- Counterfeit Part & Material Examples
- MDA Contractor Audits
- Included as Appendix A of TOR 2014-02200
Counterfeit Avoidance & Risk Mitigation

- Definition(s)
- The Risk
- U.S. Regulatory Activity
- Counterfeit Risk Mitigation
- Supplier Engagement
- Standards & Resources
- Staying Informed
- Training Resources
- Emerging Detection
- Conclusion

Example of welded lead replacements
DARPA Shield

- SHIELD aims to develop tiny components, known as dielets, that could be added to electronics parts during manufacturing or in another trusted setting. The dielets won’t have an electronic connection to the parts—and thus wouldn’t affect their functionality—but they would have an encryption engine and sensors that would detect tampering, such as revealing an exposure to light if the device had been opened up at some point between manufacture and delivery.

- With the SHIELD program, DARPA wants to develop dependable but inexpensive hardware dielets—costing less than a penny each—that could be scanned from a handheld device or larger device for large shipments. Following a scan, a handheld device such as a smartphone would communicate with the dielet, which would then send an encrypted message with information from its sensors. That response would show if any tampering occurred.

- Over $24M in Phase 1 contracts awarded between December 2014 and February 2015.

- As of Feb 2015
  - Charles Stark Draper Laboratory $4.0M (12/2014)
  - University of Illinois $0.5M (01/2015)
  - Northrop Grumman $12.2M (01/2015)
  - SRI International $6.8M (01/2015)
  - University of California Berkley $0.7M (01/2015)

- See DARPA Broad Agency Announcement DARPA-BAA-14-16 for additional details.
DNA Marking

SIGNATURE® DNA

SigNature® DNA markers provide a unique and powerful means to authenticate originality, verify provenance, and link offenders and stolen items to crime scenes. With essentially infinite variability, individualized custom DNA sequences can be created and embedded into a range of host carriers such as ink, varnish, thread, laminates and metal coatings. Highly secure, robust, durable and cost-effective, SigNature DNA markers can be used as a forensic complement to barcodes, watermarks, holograms, RFIDs, microdots or any other security platform.

SigNature DNA markers are based on full, double-stranded plant DNA. These engineered marks have not and cannot be broken. The conventional process used to sequence (“decode”) native DNA is not possible with the engineered mark. Additional layers of protection and complexity are added to the mark in a proprietary manner. This botanically engineered solution is shielded by a portfolio of 24 patents, 58 patent applications, and other intellectual property protection.
RF Emissions Analysis

Advanced Detection of Electronic Counterfeits (ADEC)

ADEC passively captures Electromagnetic (EM) signatures radiated by electronic components in order to automatically detect and identify counterfeit components. The ADEC System counterfeit detection modality is highly autonomous; non-contact and non-invasive; and has a high confidence rate of detection of counterfeits with a low false positive rate. Through early detection and screening of counterfeit parts the ADEC System prevents system failures, significant delays and redesigns and cost escalation. Updates and additions to the ADEC component signature library require a simple software upgrade and are fast and secure.

The Advanced Detection of Electronic Counterfeits (ADEC) System consists of two primary components: The ADEC Sensor and the Integrated Antenna Enclosure (IAE). Key Benefits of the ADEC System include:
- Detects electronic counterfeits and verifies part authenticity
- Detects anomalies in parts
- Enhances military capability by removing substandard electronics from weapon systems
- Prevents system failures, significant delays and redesigns and cost escalation

http://www.nokomisinc.com/ade.html
Surface Analysis

"Tag-less" track and trace solution
Mitigate threats from counterfeit items in your supply chain.
Addresses the six high-risk Federal Supply Groups (FSG’s) identified by the US Defense Logistics Agency.

- Electrical and Electronic Components (FSG 59)
- Engine Accessories (FSG 29)
- Pipe, Tubing, Hose, and Fitting (FSG 27)
- Hardware and Abrasives (FSG 53)
- Vehicular Equipment Components (FSG 25)
- Bearings (FSG 31)

BROAD APPLICABILITY

Value Proposition
Based on mature image capturing optical technique
- Non-contact and “tag-less” – avoids handling and warranty issues
- Rapid on-site enrollment/authentication
- Easy to operate; requires minimal training
- Integrate easily with manufacturing workflows (high and low throughput)
What is Battelle Barricade™?

Electronic Component Authentication Software and Data Repository

Signal Processing Software and Classifier Algorithm

Authenticated Components and Counterfeits/Clones Data Repository

Remote Server

Customer Fire Wall

To secure authentication process

To protect customer proprietary info

Customer Sites

- OEM pre-assembly verification
- OCM brand protection and QA
- Component distributor validation
- Maintenance and repair depots
- Critical points in supply chain for chain of custody assurance
- Forensic laboratories

Electronic Component Signal Acquisition Hardware and Software

Device Specific Personality Boards and Chip Sockets

Enrolled Customer Bill of Materials
Counterfeit Avoidance & Risk Mitigation

- Definition(s)
- The Risk
- U.S. Regulatory Activity
- Counterfeit Risk Mitigation
- Supplier Engagement
- Standards & Resources
- Staying Informed
- Training Resources
- Emerging Detection
- Conclusion

Example of welded lead replacements
Why are Brokers Used?

- Unaware of Risk
- Better Lead Time
- Who is Franchised
- More Responsive
- Supplier Not in System
- Parts are Obsolete
- Purchase History
- Provide Additional Services
- No Minimum Buy
- One Order vs Many

Risky Business
Why is a Broker Used?

The Item is Obsolete
Main Take Aways

- Awareness & Training
- Obsolesce Management.
- Procure ONLY from OM / OM franchised.
- Sub tier awareness, flow down and process effectiveness.
- Broker procurements ONLY when OM / Franchised no longer support.
- Know if Broker material is going to be used.
- Broker procurements MUST have robust risk mitigation.
Conclusion

- Regulatory environment evolving
- Focus on counterfeit risk avoidance
- Partnering vital to success
- Standardization, processes, reporting
- Companies aligning with regulations
- U.S. DoD, industry working on standards, prevention

Partnering Across Industry for Mutual Success