Preventing and Detecting Counterfeit Electronic Components In the Supply Chain

Henry Livingston
Technical Director & Engineering Fellow
BAE Systems Electronic Systems

This briefing includes information from publicly available documents and information used with permission from the sources.
In the news …

“EU, U.S. vow crackdown on computer counterfeits”
Reuters—Feb 22, 2008

“Fake Parts Are Seeping Into Military Aircraft Maintenance Depots”

“Counterfeit Parts Pose an Unknown Risk To Legacy Weapon Systems”
Inside the Air Force—April 25, 2008

“Three California Family Members Indicted in Connection with Sales of Counterfeit High Tech Parts to the U.S. Military”
USAO Public Affairs—9 October 2009

“Senators Carper, Brown Urge Administration to Address Counterfeit Parts Infiltrating DOD Supply Chains”
August 2010

“Counterfeit Integrated Circuits Sold to U.S. Navy and Defense Contractors”
USAO Public Affairs—14 September 2010
What is a counterfeit component? …
An Aerospace and Defense equipment manufacturer’s view

- Counterfeit components can jeopardize the performance and reliability of defense / aerospace hardware

- **Definition** …
  A suspect part that is a copy or substitute without legal right or authority to do so or one whose material, performance, or characteristics are knowingly misrepresented by a supplier in the supply chain. …
  - Do not contain the proper internal construction (die, manufacturer, wire bonding, etc.) consistent with the ordered part.
  - Used, refurbished or reclaimed, but represented as new product.
  - Different package style or surface plating/finish than the ordered parts.
  - Have not successfully completed the Original Component Manufacturer’s (OCM)’s full production and test flow, but are represented as completed product.
  - Upscreened parts, which have not successfully completed upscreening.
  - Modified labeling or markings intended to misrepresent the part’s form, fit, function, or grade.

From SAE Aerospace Standard AS5553
Causal factors / vulnerabilities

- Reduced impact of Aerospace & Defense on global component market

- Aerospace & Defense product cycle longer than the manufacturing life of the electronic components used in those products (i.e. DMSMS)

- e-Waste — Component Salvaging & Reprocessing

- Sourcing via Internet

- Component manufacturing practices
  - Outsourcing oversight
  - Scrap and disposal

- Themes from the US Dept. of Commerce Counterfeit Electronics Study
  - Less stringent inventory management by Brokers and Independent Distributors
  - Greater reliance on gray market parts by Brokers, Independent Distributors and Contract Manufacturers
  - Insufficient chain of accountability
  - Purchase of excess inventory on open market
  - Insufficient buying procedures
  - Inadequate purchase planning by OEMs and Contract Manufacturers
e-Waste — feedstock for counterfeiters
Procurement practices can create vulnerabilities

FBI places much of the blame on government acquisition practices

FBI Criminal Investigation: Cisco Routers

The Threat

- IT Subversion/Supply Chain Attack
  - Cause immediate or premature system failure during usage
  - Gain access to otherwise secure systems
  - Weaken cryptographic systems
- Requires “intimate access to target system”

Government Procurement

- Government searches for lowest price
- Contract language allows for
  - Subcontracts
    - 2 to 3 levels of sub-contractors
  - “Blind drop” or “drop ship”
  - Non-OEM purchase
  - Smaller businesses
- No vetting of vendors by Cisco or GSA
  - If done by government, usually only background check

FBI Criminal Investigation — Cisco Routers
Jan 11, 2008
www.stopfakes.com
“Three California Family Members Indicted in Connection with Sales of Counterfeit High Tech Parts to the U.S. Military”
USAO Public Affairs—9 October 2009

• Three members of a California family have been charged with selling counterfeit integrated circuits to the Navy and other government agencies.

  • … imported integrated circuits bearing counterfeit trade marks, including military-grade markings …

  • … obtained trademark-branded integrated circuits from unknown sources, and then scraped, sanded, or ground off the original markings, repainted and remarked the devices with another trademark thereby fraudulently indicating, among other things, that the devices were of a certain brand, newer, higher quality, or were of military grade.

• "This case highlights the significant potential impact such crimes also can have on public health and safety as well as national security."
“Counterfeit Integrated Circuits Sold to U.S. Navy and Defense Contractors”
USAO Public Affairs—14 September 2010

- Owner and employee of Florida-based company indicted in connection with sales of counterfeit high tech devices destined to the U.S. Military and other Industries …
  - … imported counterfeit integrated circuits from China and Hong Kong and sold them to the U.S. Navy, defense contractors and others, marketing some of these products as “military-grade.”
  - “This case shows our determination to work in coordination with our law enforcement partners and the private sector to aggressively prosecute those who traffic in counterfeit parts.”
Defense Industrial Base Assessment: COUNTERFEIT ELECTRONICS
U.S. Department of Commerce Bureau of Industry and Security (January 2010)

- All elements of the supply chain have been directly impacted
- Lack of dialogue between all organizations in the U.S. supply chain
- Organizations assume that others are testing parts
- Lack of traceability in the supply chain
- Insufficient chain of accountability within organizations
- Very limited recordkeeping on counterfeit incidents
- Most organizations do not know whom to contact in the U.S. Government
- Stricter testing protocols and quality control practices for inventories are required
- Most DOD organizations do not have policies in place to prevent counterfeit parts from infiltrating their supply chain
DOD does not currently have a policy or specific processes for detecting and preventing counterfeit parts.

- Existing procurement and quality-control practices used to identify deficient parts are limited in their ability to prevent and detect counterfeit parts in DOD's supply chain.

Individual commercial sector companies have developed a number of anticounterfeiting measures, including increased supplier visibility, detection, reporting, and disposal.

Recent collaborative industry initiatives have focused on identifying and sharing methods to reduce the likelihood of counterfeit parts entering the supply chain.

Agency officials have an opportunity to leverage knowledge and ongoing and planned initiatives to help mitigate the risk of counterfeit parts as DOD develops its anticounterfeiting strategy.
Senators Carper, Brown Urge Administration to Address Counterfeit Parts Infiltrating DOD Supply Chains
(August 2010)

• “Both the Department of Commerce and GAO report offer little reassurance that the Defense Supplier Base is secure from the risks of counterfeit parts.”

• “In fact, both reports note that federal agencies, including those within the DOD, do not have effective policies or specific processes in place for detecting, tracking and preventing the use of counterfeit parts.”

• “In the absence of effective prevention measures including testing, vetting of suppliers, and data collection and analysis, as well as concerted enforcement efforts, the current supply system is not adequately addressing the risks to national security from counterfeit parts.”

• “Our understanding is that the Department of Defense will establish guidance, including consistent practices for preventing, detecting, reporting, and disposing of counterfeit parts, later this year.”

Letter to Honorable Ashton B. Carter, Under Secretary of Defense for Acquisition, Technology & Logistics (6 August 2010)
Defense Industrial Base Assessment:
COUNTERFEIT ELECTRONICS
U.S. Department of Commerce Bureau of Industry and Security (January 2010)

May 5, 2009

Counterfeits and the U.S. Industrial Base

Counterfeit Electronics Study -Goals
- Assess the impact of counterfeit electronics on U.S. supply chain integrity, critical infrastructure, and industrial capabilities
- Recommend best practices to mitigate risk to U.S. supply chain
- Study sponsored by Naval Air Systems Command with support from Semiconductor Industry Association (SIA)

Counterfeit Electronics Study -OTE surveys distributed
- 5 separate but related surveys targeting:
  - Microchip & discrete electronic manufacturers – 106
  - Electronic board producers/assemblers – 37
  - Distributors and brokers of electronic parts – 144
  - Prime contractors and subcontractors – 147
  - DOD arsenals, depots, and DLA – 64
- 498 total survey participants

© 2010 BAE Systems
All Rights Reserved
Counterfeit incidents are increasing

Total Counterfeit Incidents: OCMs, Distributors, Board Assemblers, Prime/Sub Contractors 2005 - 2008

U.S. Department of Commerce – Preliminary Data (as of March 4, 2009)

> 140% increase

U.S. Department of Commerce Bureau of Industry and Security
Vast majority of counterfeit cases are not reported.

Counterfeit Reporting
Parts & Documents

DOC/BIS survey reports more than 9,000 counterfeit incidents in 2008.

Reasons for Not Reporting to GIDEP:
- "We are unaware of reporting agencies. We would be happy to participate if we were aware of these programs."
  - Independent Distributor
- Reporting to GIDEP will inaccurately "show that our company has no control over purchasing operations by buying counterfeit products."
  - Independent Distributor

Percent of Companies With Counterfeits Reporting to GIDEP:
- Report 18%
- Do Not Report 82%
Top source and suppliers of counterfeits

Top source of counterfeits … - China
Top suppliers of counterfeits … - Brokers - Independent Distributors

Who is Selling Counterfeits?*

* Only includes companies that encountered counterfeits

U.S. Department of Commerce
Bureau of Industry and Security

* Each company was asked to provide their top five suspected countries

U.S. Department of Commerce – Preliminary Data (as of March 4, 2009)
In production vs. out of production products

Robust procurement practices and planning can avoid 50% of the problem, but …

Many use a source other than the OCM or its authorized distributor:
- Small quantity buys
- Parts with long lead times

Obsolete parts present the greatest vulnerability (not available from authorized sources)

U.S. Department of Commerce – Preliminary Data (as of March 4, 2009)

U.S. Department of Commerce
Bureau of Industry and Security
Resources applied to combat counterfeits

Full-Time Employees (FTEs) Dedicated to Counterfeit Issues

<table>
<thead>
<tr>
<th>Year</th>
<th>Number of FTEs</th>
</tr>
</thead>
<tbody>
<tr>
<td>2005</td>
<td>266</td>
</tr>
<tr>
<td>2006</td>
<td>314</td>
</tr>
<tr>
<td>2007</td>
<td>404</td>
</tr>
<tr>
<td>2008 est.</td>
<td>500</td>
</tr>
</tbody>
</table>

Number of Companies With At Least One FTE Dedicated to Counterfeit Issues (2008 est.)

<table>
<thead>
<tr>
<th>Category</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distributors</td>
<td>64%</td>
</tr>
<tr>
<td>Circuit Board Assemblers</td>
<td>34%</td>
</tr>
<tr>
<td>Prime/Sub Contractors</td>
<td>28%</td>
</tr>
<tr>
<td>OCMs</td>
<td>27%</td>
</tr>
</tbody>
</table>

U.S. Department of Commerce – Preliminary Data (as of March 4, 2009)

Most prime / subcontractors and assembly producers do not apply sufficient resources to combat the problem

U.S. Department of Commerce Bureau of Industry and Security
DOD material procurement vulnerabilities

DOD Identification of Counterfeits

Comments:
- "Once [parts] reach the shop floor they are assumed to be legitimate and are only discovered if they fail."
  - Non-DLA Organization
- "The process for identification of counterfeit parts is undefined."
  - Non-DLA Organization
- "Our inspectors do not inspect to the degree that would normally identify counterfeit electronics."
  - DLA Organization

Percent of DOD Organizations Who Find It Difficult to Identify Counterfeit Parts

DLA and DOD Arsenals & Depots may not be equipped to address the problem

Internal Actions Taken to Prevent Infiltration of Counterfeits - DOD

<table>
<thead>
<tr>
<th>No internal actions taken</th>
<th>DLA Organizations</th>
<th>Non-DLA Organizations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Performing screening and testing on inventory</td>
<td>83%</td>
<td>59%</td>
</tr>
<tr>
<td>Training staff on the negative economic and safety impact of counterfeet products</td>
<td>17%</td>
<td>24%</td>
</tr>
<tr>
<td>Revising organization procedures for disposal of &quot;seconds,&quot; defective parts, and production overruns</td>
<td>11%</td>
<td>21%</td>
</tr>
<tr>
<td>Revising procurement to more carefully screen/audit/evaluate authorized returns from customers</td>
<td>11%</td>
<td>14%</td>
</tr>
<tr>
<td>Adding security markings to existing inventory</td>
<td>6%</td>
<td>10%</td>
</tr>
<tr>
<td>Embedding new security measures in existing product lines</td>
<td>6%</td>
<td>0%</td>
</tr>
<tr>
<td>Embedding new security measures in product lines</td>
<td>0%</td>
<td>0%</td>
</tr>
</tbody>
</table>

U.S. Department of Commerce – Preliminary Data (as of March 4, 2009)
Observations From Counterfeit Detection Experiences

Henry Livingston, BAE Systems Electronic Systems
Introduction

- BAE Systems Electronic Systems issued eighteen (18) GIDEP Alerts from December 2006 to July 2007 reporting suspect counterfeit parts.

- This briefing presents observations from these examples …
  - Case summaries and supply chain analysis
  - Observations from counterfeit detection efforts

- Our findings drove …
  - Changes to BAE Systems Electronic Systems procurement practices and methodology for detecting counterfeits
  - BAE Systems Electronic Systems contributions to new industry standards designed to combat the counterfeit parts problem


## Counterfeit case summaries

<table>
<thead>
<tr>
<th>GIDEP Alert</th>
<th>Findings …</th>
</tr>
</thead>
<tbody>
<tr>
<td>J5-A-07-01</td>
<td>Parts marked as Philips QML product with 2003 date code, but contained Intel die manufactured in 1980</td>
</tr>
<tr>
<td>J5-A-07-02</td>
<td>Parts marked as Analog Devices QML product, but markings were not consistent with standard Analog Devices markings for the device and device contained die of a different function</td>
</tr>
<tr>
<td>J5-A-07-03</td>
<td>Parts marked as Cypress commercial product, but parts were salvaged from scrapped assemblies</td>
</tr>
<tr>
<td>J5-A-07-04</td>
<td>Received parts Jan-06 thru May-06 marked as On Semiconductor commercial product, but On Semiconductor did not manufacture these parts</td>
</tr>
<tr>
<td>J5-A-07-05 &amp; J5-A-07-07</td>
<td>Received parts marked as Seeq commercial product, but parts were salvaged from scrapped assemblies and remarked to appear as legitimate/unused product</td>
</tr>
<tr>
<td>J5-A-07-06</td>
<td>Parts marked as Philips QML product with 9852 date code, but Philips discontinued manufacture 31 December 1997</td>
</tr>
<tr>
<td>J5-A-07-08</td>
<td>Parts marked as National QML product, but major discrepancies in marking format and content, including date code and manufacturing location; Die contained in these parts were not manufactured by National Semiconductor</td>
</tr>
<tr>
<td>J5-A-07-09</td>
<td>2001 date code, but Intersil discontinued this product in 2000; marking missing country of origin; parts had wrong lead finish</td>
</tr>
<tr>
<td>J5-A-07-10</td>
<td>2004 date code, but Linear Tech discontinued this product in 2001</td>
</tr>
<tr>
<td>J5-A-07-11A</td>
<td>Parts marked as Analog Devices QML product, but incomplete or absent marking; incorrect lead finish vs part number; reclaimed or refurbished; invalid test report</td>
</tr>
<tr>
<td>J5-A-07-12</td>
<td>Part number and date code do not match the lot number identified in Cypress production records</td>
</tr>
<tr>
<td>J5-A-07-13</td>
<td>Suspect marking; evidence of marking; part number and date code do not match Cypress lot number</td>
</tr>
<tr>
<td>J5-A-07-14</td>
<td>Parts marked as Analog Devices &quot;883&quot; product, but incomplete or absent marking; incorrect lead finish vs part number; reclaimed or refurbished; invalid test report; evidence of prior marking</td>
</tr>
<tr>
<td>J5-A-07-15</td>
<td>Parts marked as Cypress commercial product; leads have been re-soldered; evidence of a resurfacing on device package</td>
</tr>
<tr>
<td>J5-A-07-16</td>
<td>Parts marked as Xicor/Intersil QML product, but marking is not compliant to Xicor/Intersil brand layout; die not associated with QML product</td>
</tr>
<tr>
<td>J5-A-07-17</td>
<td>Discrepancies in device marking, lead finish and lead quality</td>
</tr>
<tr>
<td>J5-A-07-18</td>
<td>Parts appear to be reclaimed; the surface roughness the devices markings were stripped and remarked</td>
</tr>
</tbody>
</table>
Supply chain analysis

Parts exchange hands several times before reaching the end user.

Eight (8) out of our eighteen (18) cases trace back to sources in China… …Perhaps more.

All involve Independent Distributors

Seventeen (17) unique part types. Broad variety of device functions. Ten (10) manufacturers represented.

Twenty (20) USA based suppliers

Eleven (11) China based suppliers

Origin unknown for all cases

Similar bogus test reports

Same unique part type obtained through several suppliers.

Full details available to GIDEP Participants. Others may apply for membership at the GIDEP Help Desk (951-898-3207)

© 2010 BAE Systems
All Rights Reserved
Observations from counterfeit detection efforts

- Industry and Government inspection and test methods are designed to verify the integrity of authentic parts ... not to detect counterfeits

- Verifiable supply chain traceability to the Original Component Manufacturers typically does not exist for components acquired through the open market

- Many suppliers do not understand or seek verifiable supply chain traceability documentation

- Supply chain traceability and certification documentation may not be authentic

- Original Component Manufacturers are frequently unwilling to help authenticate components acquired through Independent Distributors

- Original Component Manufacturer production records may not be available for older parts

- Many parts show evidence of poor storage and handling conditions or termination refurbishing or reclamation
Conclusions from BAE Systems Electronic Systems experience

• Electronic equipment manufacturers and Government users must be vigilant in order to avoid counterfeit electronic components.

• The vast majority of counterfeit cases reported are associated with purchases through independent distributors.

• The most effective approach to avoiding counterfeit electronic components is to purchase product directly from …
  • the original manufacturer
  • a distributor who is franchised or authorized by the original manufacturer

• A substantial number of products are no longer available through franchised or authorized suppliers.

• Independent distributors are not all created equal.
  • Users need to understand the independent distributor’s operations and business processes.
  • Users should use mitigation methods to reduce the potential for acquiring counterfeits.
Industry Standards Gap Analysis
Henry Livingston, BAE Systems Electronic Systems
Industry standards gap analysis

Key Elements:

- **Procurement Practices:** procurement practices developed specifically to prevent the acquisition of counterfeit parts
- **Product Traceability:** methods to retain traceability of products from the original manufacturer to the end user.
- **Risk Mitigation:** approaches to assess and mitigate risks of procuring parts from riskier sources.
- **Verification / Detection:** methods applied specifically to detect counterfeits
- **Containment / Disposition:** containment and disposition guidance for use when counterfeits are discovered
- **Reporting:** reporting guidance so that both industry and US Government organizations can determine whether or not they are similarly affected

- **Component Obsolescence Management:** guidance to address component obsolescence and, therefore, reduce the likelihood of having to acquire parts through riskier suppliers

Target Users:

- System Integrators (SI)
- Original Equipment Manufacturers (OEM)
- Component Distributors (CD)
- Original Component Manufacturers (OCM)

Review of industry standards vs. key elements for counterfeit avoidance, detection, mitigation and disposition
<table>
<thead>
<tr>
<th>Standard</th>
<th>Scope</th>
<th>USER</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>International Organization for Standardization (ISO) ...</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISO 9001 Quality Management Systems - Requirements</td>
<td>Parts, Materials, Assemblies and Equipment</td>
<td>X</td>
<td>Does not cover counterfeit prevention, detection and avoidance elements</td>
</tr>
<tr>
<td><strong>SAE International ...</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SAE AS9100 Quality Systems – Aerospace – Model for Quality Assurance in</td>
<td>Parts, Materials, Assemblies and Equipment</td>
<td>X</td>
<td>Does not cover counterfeit prevention, detection and avoidance elements</td>
</tr>
<tr>
<td>Design, Development, Production, Installation and Servicing</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SAE AS9120 Quality Management Systems – Aerospace Requirements for</td>
<td>Parts, Materials, Assemblies and Equipment</td>
<td></td>
<td>Purchasing process requirements call for general</td>
</tr>
<tr>
<td>Stockist Distributors</td>
<td></td>
<td>X</td>
<td>requirement to “prevent the purchase of counterfeit/compliant unapproved products.”</td>
</tr>
<tr>
<td>SAE AS9003 Inspection and Test Quality System</td>
<td>Electronic Components</td>
<td>X</td>
<td>Does not cover counterfeit prevention, detection and avoidance elements</td>
</tr>
<tr>
<td>SAE AS5553 Counterfeit Electronic Parts; Avoidance, Detection,</td>
<td>Electronic Components</td>
<td>X</td>
<td>Released April 2009</td>
</tr>
<tr>
<td>Mitigation, and Disposition</td>
<td></td>
<td></td>
<td>DoD Adopted August 2009</td>
</tr>
<tr>
<td>SAE AS6081 (proposed) Counterfeit Electronic Parts Avoidance –</td>
<td>Electronic Components</td>
<td>X</td>
<td>Comprehensive coverage for all elements</td>
</tr>
<tr>
<td>Distributors</td>
<td></td>
<td></td>
<td>Standard development in process</td>
</tr>
<tr>
<td><strong>TechAmerica ...</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TechAmerica-TB-0003 Counterfeit Parts &amp; Materials Risk Mitigation</td>
<td>Parts and materials</td>
<td>X</td>
<td>Released February 2009 High level guidance</td>
</tr>
<tr>
<td>EIA-4899 Standard for Preparing an Electronic Components Management</td>
<td>Electronic Components</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Plan</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EIA-933 Standard for Preparing a COTS Assembly Management Plan</td>
<td>Assemblies</td>
<td>X</td>
<td>Proposed Rev A requires a “Counterfeit Electronic Parts Control Plan” for flight critical assemblies</td>
</tr>
<tr>
<td>EIA-GEB1 Diminishing Manufacturing Sources and Material Shortages (DMSMS)</td>
<td>Parts, Materials, Assemblies and Equipment</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>-------------------------------------------------------------------------</td>
<td>------------------------------------</td>
<td>------</td>
<td>----</td>
</tr>
<tr>
<td>Federal Aviation Administration (FAA) ...</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FAA AC 00-56 Voluntary Industry Distributor Accreditation Program</td>
<td>Parts, Materials and Assemblies</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPC ...</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPC-175X (proposed) Requirements for Best Practices Procurement Procedures (Counterfeit Avoidance)</td>
<td>Parts and Materials</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>JEDEC ...</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>JEDEC01 General Requirements for Distributors of Commercial and Military Semiconductor Devices</td>
<td>Semiconductor Components</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Independent Distributors of Electronics Association (IDEA) ...</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IDEA-STO-1010 Acceptability of Electronic Components Distributed in the Open Market</td>
<td>Electronic Components</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Semiconductor Equipment and Materials International (SEMI) ...</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEMI T20 System Architecture for Preventing/Detecting Semiconductor Counterfeit Products</td>
<td>Semiconductor Components</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>SEMI XX Specification for Object Labeling to Authenticate Semiconductors and Related Products In An Open Market</td>
<td>Semiconductor Components</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>SEMI YY Guide for Qualifications of Authentication Service Bodies for Detecting and Preventing Counterfeiting Of Semiconductors and Related Products</td>
<td>Semiconductor Components</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Electronic Components, Assemblies and Materials Association (ECA) ...</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EIA/ECA-CB21 Counterfeit Passive Components</td>
<td>Passive Components</td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

November 2010 - 28
Gap analysis observations

• **Poor coverage in high level standards** for Quality Management Systems (QMS)
  - QMS standards do not address key elements required for a robust counterfeit avoidance program
  - Industry organizations involved in maintaining key US and international QMS standards have yet to initiate definitive steps to embed counterfeit avoidance elements into...
    - QMS standards
    - supplier certification programs

• **Excellent coverage in lower level standards** for electronic components for use by:
  - Original Component Manufacturers (OCMs) to establish a means to track and authenticate components throughout the supply chain
  - Component Distributors (CDs) and Original Equipment Manufacturers (OEM) to track and authenticate current production components throughout the supply chain (obsolete parts remain vulnerable to lack of supply chain traceability)
  - Original Equipment Manufacturers (OEM) and System Integrators (SI) to avoid introducing counterfeit components within their products

• **Major emphasis on semiconductor components**
  … the subject of most counterfeiting reports over the past few years
SAE Aerospace Standard AS5553 – Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition

- Released April 2009
- Adopted for use by DOD August 2009
- Requirements, practices & methods …
  - Parts Availability
  - Purchasing / Purchasing Information
  - Verification of Purchased Product / In Process Investigation
  - Material Control
  - Reporting
### Industry standards gap analysis

#### Key Elements:
- **Procurement Practices:** Procurement practices developed specifically to prevent the acquisition of counterfeit parts.
- **Product Traceability:** Methods to maintain traceability of products from the original manufacturer to the end user.
- **Risk Mitigation:** Approaches to assess and mitigate risks of procuring parts from riskier sources.
- **Verification / Detection:** Methods applied specifically to detect counterfeits.
- **Containment / Disposition:** Containment and disposition guidance for use when counterfeits are discovered.
- **Reporting:** Reporting guidance so that both industry and US government organizations can determine whether or not they are similarly affected.
- **Component Obsolescence Management:** Guidance to address component obsolescence and, therefore, reduce the likelihood of having to acquire parts through riskier suppliers.

#### Target Users:
- System Integrators (SI)
- Original Equipment Manufacturers (OEM)
- Component Distributors (CD)
- Original Component Manufacturers (OCM)

BAE Systems Electronic Systems policies and practices include all key elements.
BAE Systems Electronic Systems policies and practices include all key elements to avoid counterfeit parts …

• Specify a preference for procurement from …
  • Original Equipment Manufacturers (OEMs),
  • Original Component Manufacturers (OCMs) or
  • Authorized/franchised distributors

• Independent Distributors are used only when parts are not available from OEMs, OCMs or authorized/franchised distributors
  • Documented search for OEMs, OCMs and franchised/authorized distributors
  • Use of Independent Distributors after consideration of alternate parts, re-design, schedule adjustments and a reasonable
  • Purchases made from Independent Distributors who have been thoroughly vetted and approved for use
BAE Systems Electronic Systems policies and practices include all key elements to avoid counterfeit parts …

• Due diligence applied when procuring from Independent Distributors…
  • Purchase order quality assurance clausing and other terms and conditions.
  • Specific inspection requirements
  • Third party and in-house validation and testing requirements
  • Certificates of conformance, certificates of origin and other documentation to support the authenticity of the parts

• Counterfeit parts avoidance requirements are flowed down to suppliers on all purchase orders and subcontracts
  • Flowdown does not always yield compliance
  • Awareness training and auditing is necessary to ensure understanding of the issue and assure compliance via process
BAE Systems Electronic Systems policies and practices include all key elements to avoid counterfeit parts …

• Confirmed suspect counterfeit parts processed in accordance with Non-Conforming Product procedures

• Prompt reporting of counterfeit parts to:
  • Customers
  • DCMA, other equivalent national agencies, as appropriate (e.g., GIDEP)
  • Other BAE Systems business entities
Preventing and Detecting Counterfeit Parts In the Supply Chain

... a case study

Henry Livingston, BAE Systems Electronic Systems
“Counterfeit Integrated Circuits Sold to U.S. Navy and Defense Contractors”
USAO Public Affairs—14 September 2010

- Owner and employee of Florida-based company indicted in connection with sales of counterfeit high tech devices destined to the U.S. Military and other Industries …

- … imported counterfeit integrated circuits from China and Hong Kong and sold them to the U.S. Navy, defense contractors and others, marketing some of these products as “military-grade.”

- “This case shows our determination to work in coordination with our law enforcement partners and the private sector to aggressively prosecute those who traffic in counterfeit parts.”
“Counterfeit Integrated Circuits Sold to U.S. Navy and Defense Contractors”
USAO Public Affairs—14 September 2010

• … numerous customer complaints regarding the counterfeit integrated circuits sold by the defendants and others …

• One event associated with BAE Systems and the Naval Air Warfare Center Aircraft Division (NAWCAD) ….

“An August 2007 sale of 75 counterfeit National Semiconductor Corporation ICs to a company in California that was fulfilling a joint contract with BAE Systems Technology Solutions & Services and the Naval Air Warfare Center Aircraft Division (“NAWCAD”), Detection and Surveillance Branch, Integrated Logistics Engineering. The ICs were intended to be used for production of ship-based antenna equipment, the Identification Friend Foe (“IFF”) system, which is used to determine an airplane’s identification and intentions while in flight.”
A case study in DOD – industry collaboration

- The DOD supply chain environment …
  - The original component manufacturer of these parts discontinued production of this product in 1993.
  - The only suppliers offering these parts were independent distributors and brokers.
  - Schedule and funding constraints did not allow for design changes necessary to eliminate the obsolete part.
A case study in DOD – industry collaboration

- Due diligence, detection and containment …

  - BAE Systems recommended to NAWCAD that it apply counterfeit avoidance practices developed by BAE Systems.
    - These counterfeit avoidance practices are the same found in SAE Aerospace Standard AS5553 – Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition.

  - The counterfeit detection procedure included within these practices revealed that the parts were suspect counterfeit.

  - BAE Systems discussions with the original component manufacturer confirmed that the parts were counterfeit.

  - The counterfeit parts were immediately segregated and quarantined, and did not re-enter the DOD supply chain.
A case study in DOD – industry collaboration

• Reporting …

  • BAE Systems initiated a GIDEP Alert on behalf of the Navy to notify government and industry of this finding.

  • NAWCAD notified the Naval Criminal Investigative Service (NCIS) of this counterfeit part incident.

  • The GIDEP Alert submitted by BAE Systems prompted NCIS to refer the case to the US Department of Justice for further investigation and prosecution.
A case study in DOD – industry collaboration

• This event is an example of how collaboration between DOD and industry can effectively combat counterfeit electronic components:

1. When purchases from sources of supply other than the original component manufacturer and its authorized distribution chain are necessary, due diligence must be performed to avoid counterfeits.

2. When counterfeits are discovered, steps must be taken to avoid reintroducing counterfeits into the supply chain.

3. US Government agencies, contractors, and lower tier suppliers should promptly communicate their findings of counterfeits they encounter.
Conclusion

• Industry and US Government procurement activities may effectively combat counterfeit electronic components by undertaking three steps:

1. Apply supplier preferences for electronic components purchased from original manufacturers or their authorized distributors.
   • Flow down counterfeit avoidance requirements to suppliers

2. Perform due diligence to avoid counterfeits when purchases from sources of supply other than the original component manufacturer and its authorized distribution chain are necessary.

3. Notify Government and industry of suspect counterfeits when they are encountered.
   • Review information/reporting sources (e.g., GIDEP) to keep abreast of what others in Government and industry are finding and reporting
Our customers

We Protect Those Who Protect Us®