Counterfeit Prevention in the DoD: A Technical Perspective

Mr. Nicholas M. Torelli
Director, Mission Assurance
Office of the Deputy Assistant Secretary of Defense for Systems Engineering

SAE 2012 Counterfeit Parts Avoidance Symposium
Phoenix, AZ | November 2, 2012
Systems Engineering

• To make good acquisition decisions, we need to understand and manage, in a deep way, the myriad technical risks involved in designing, developing and delivering some of the most complex systems ever deployed

• Systems Engineering focuses on engineering excellence – the creative application of scientific principles:
  – To design, develop, construct and operate complex systems
  – To forecast their behavior under specific operating conditions
  – To deliver their intended functions while addressing economic efficiency, environmental stewardship and safety of life and property.

• Systems Engineering is both a technical and a management discipline
Systems Engineering Challenges

- Start programs right with strong early SE
- Perform robust reliability and maintainability engineering
- Emphasize design for manufacturing
- Create the tools to support rapid capability delivery
- Reinvigorate Defense Standardization
- Expand the aperture of DoD engineering practice to address 21st century technical challenges

All of these must be considered in how we address Counterfeit Prevention
Globalized Industrial Base

Industrial foundation becoming more integrated between the U.S., its allies, and global commercial markets

Growing dependence upon international commerce
Globalization of the Semiconductor Industry

- U.S. holds 48% semiconductor market share (sales)
- But . . . manufacturing capacity went from 25% (2005) to 14% (2009)
- Large portion of off-shore investment made by U.S. Corporations
- But . . . disproportionately low investment in U.S. capacity

If each region’s size reflected its investment in new semiconductor equipment, Japan and Taiwan would be larger than North America, and Korea would be close.

U.S. Losing Share in New Semiconductor Manufacturing Capacity

Chart 6: The Share of World Capacity Has Grown in Korea, Taiwan and China but Has Fallen in Japan, the United States and Europe

Source: SEMI Industry Research & Statistics Department. Data beyond 2005 Q1 based on projections.
Profile of Counterfeit Risk

- Most preferred source for critical items
- Approved manufacturing and test process
- Systems engineering and QA program
- Specifications authenticated and original
- Passed DOD audits, documentation trail

- Parts are no longer produced by OEMs
- Suppliers have ability to demonstrate documentation traceability and conformance to specifications
- Demonstrate technical accountability
- Strong inventory and record keeping

- Minimal background on supplier capabilities
- Technical and business expertise unverified
- Company parts sources unknown

Prolonged use of aging systems creates opportunities for counterfeit parts to enter the supply chain
Focus—Detection and Avoidance of Counterfeit Electronic Parts

Tenets:

- Directs DOD to assess current anti-counterfeiting practices and implement “risk-based” policies to address counterfeit
- Requires DOD and contractors whenever possible to buy electronic parts from the Original Component Manufacturer (OCM) or its authorized distributor(s)
- Directs DOD to establish a “Trusted Supplier” program to certify organizations that comply with industry standards on anti-counterfeiting
- Institutes cost recovery for counterfeit items
- Re-affirms mandatory reporting (GIDEP) for incidents internal and external to DOD
- Requires the Secretary of Homeland Security to establish a methodology for the enhanced inspection of electronic parts after consulting with the SECDEF as to the sources of counterfeit parts in the defense supply chain

Specific Actions:

- Establish DOD-wide definition
- Issue anti-counterfeit mitigation guidance
- Issue remedial action guidance
- Create reporting process (GIDEP)
- Develop process to analyze and act on reports
- Incorporate in DFAR anti-counterfeit language
Counterfeit Problem Space

• **Counterfeits for Profit:**
  – Up-screened, re-marked, or re-used parts sold as new/authentic
  – Avoidable through OEM procurement; most should be detectable with sufficient inspection or test

• **Counterfeits for Malice:**
  – “Perfect” parts that also perform additional, unwanted functions
  – Designed to pass inspection
  – Must be combated with intelligence, Operational Security (OPSEC), and enhanced test & evaluation (T&E)

Counterfeits impact DoD safety, mission, and costs regardless of the motivation, but the techniques for combating them vary by motive.
USD(AT&L) Memorandum: Overarching Counterfeit Prevention Guidance

- Addresses an area of critical concern while Department policy is in coordination
- Provides definition
- Emphasizes
  - Risk-based approach
  - Leverages Program Protection Plan and non-conforming processes
  - Directs use of contracting clauses and data elements to ensure traceability and reporting on critical items for contractors and subcontractors
  - Use of anti-counterfeiting standards
  - Disposal of counterfeit items
  - Training
Risk-based Counterfeit Prevention Strategy

• Determine the risk posed if a part were identified as counterfeit
  • Product Risk (the criticality of the product in which the part will be used)
  • Component Risk (the risk to the product that is associated with the failure of the part/component)
  • Supplier Risk (the risk incurred due to use of a selected manufacturer or distributor)

• Broadly, gains can be made by evolving industry and supplier business practices for counterfeit avoidance and detection
  • Raise the bar for industry and DoD counterfeit avoidance and detection

• For mission-critical and safety-critical components, apply enhanced mitigations
  • Trusted Defense Systems Strategy

Prevention ✧ Detection ✧ Remediation ✧ Reporting ✧ Restitution
The DoDI 5000.02 Process
Detection - Identification - Disposition

**Counterfeit Part Detection**
- Materiel control and traceability program
- Quality management systems
- Systemic test and verification processes

**Identification**
- Use product quality deficiency reporting processes
- Conduct engineering analysis and authenticity determination
- Report in GIDE�

**Disposition**
- Hold for law enforcement disposition
- Dispose according to federal logistics information system code guidance
- Execute suspension and debarment process as required

**DoD Policy standardizing processes across supply chain**
Non-Conformances

Parts/Assemblies

Non-Conforming

Quality Stuff !!!

“Honest” Quality Deficiency

Malicious Intent

Counterfeit

Dishonest

Fraud (for Profit)

For Profit
Gov’t Acceptance – “The Dividing Line”
(that really does not matter)

Government Possession

Major Acquisition
System Prime

Warfighter
Depot Maintenance
Prime Vendor Depot Support
Defense Logistics
Supplier
Integrator
Supplier
Integrator
Supplier
Supplier
Supplier
Supplier
Supplier
Supplier
Supplier

Industry Possession

Government Industry Data Exchange Program
Product Deficiency Reporting & Evaluation Program
Key Implementation Activities

Risk-based technical approach to lessen the impact of counterfeits

• **Acquisition Policy, Guidance, and Oversight**
  – Defense Acquisition Guidebook (DAG)
  – Systems Engineering Plan (SEP)

• **Program Protection Planning**
  – Supply Chain Risk Management
  – System Security Engineering

• **GIDEP information system; rules, regulations, reporting**

• **“Trustworthiness” of Suppliers**
  – Defense Microelectronics Agency (DMEA) “Trusted” Supplier Program
  – DLA QSL/D*
  – Industry designated suppliers
  – Inspection and Test philosophy

*Qualified Supplier List / Distributor*
### Technical Schedule

#### Certification Requirements

#### Technical Review Criteria

#### Design Considerations

### Engineering Tools

#### Risks, Issues, and Opportunities
## Counterfeit Prevention: Select DAG Chapter 4

### Design Consideration Correlations

<table>
<thead>
<tr>
<th>Design Consideration</th>
<th>Relationship</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reliability &amp; Maintainability Engineering</td>
<td>Counterfeits that somehow get past receipt inspection and test can have radically different reliability and failure modes than the “honest” part.</td>
</tr>
<tr>
<td>Critical Safety Items</td>
<td>From an Anti-Counterfeiting Risk Based Approach, CSI are going to be more carefully scrutinized (inspected / tested) to ensure no counterfeits infiltrate supply.</td>
</tr>
<tr>
<td>ESOH</td>
<td>RoHS has driven increased number counterfeits where a lead-free microcircuit is sold as have tin-lead leads.</td>
</tr>
<tr>
<td>Corrosion Prevention and Control</td>
<td>Counterfeits, by their nature, may have falsely certified CPC. Additionally, if the counterfeit is a compound or component (e.g. gaskets; ground wires) intended to prevent or reduce corrosion, the effects may appear long before the predicted times and the impacts can be far worse.</td>
</tr>
<tr>
<td>Supportability</td>
<td>Increased failure rates can turn out to be due to counterfeits; unexplained failures can negatively impact supportability and might drive incorrect problem resolution behaviors.</td>
</tr>
</tbody>
</table>
### Design Consideration Correlations (cont.)

<table>
<thead>
<tr>
<th>Design Consideration</th>
<th>Relationship</th>
</tr>
</thead>
<tbody>
<tr>
<td>Commercial-Off-the-Shelf</td>
<td>The government and its industry agents will have considerably less visibility into the supply chains that create COTS products. An implication of this is counterfeit vulnerabilities as described in the other design consideration sections of this table.</td>
</tr>
<tr>
<td>DMSMS</td>
<td>As systems age and the trustworthy sources for the piece parts dry up, counterfeiters increasing take advantage of the situation by offering sources for hard-to-find-parts.</td>
</tr>
<tr>
<td>Disposal and Demilitarization</td>
<td>D&amp;D is an excellent source for counterfeiters to obtain parts that can be turned into “used sold as new” parts (fraudulently certified as new).</td>
</tr>
<tr>
<td>Open Systems Architecture</td>
<td>OSA could provide a means to quickly certify a newer, more available part for use in weapon systems, thus reducing the impact of DMSMS. Conversely, it could also result in more part numbers (equivalents) being introduced into supply thus increasing the likelihood of counterfeit intrusion.</td>
</tr>
</tbody>
</table>
A business decision based on technical, industrial base, and supply chain factors

- **Orig. Comp. Mfg. Auth. Distr.**
- **Auth. Distr. Broker/Distributor**
- **Prime**
- **Depot**
- **Acquisition Phase (New)**
- **Sustainment/Legacy Phase (Old - DMSMS)**

**Trust In Supply**
During Design

• **Engineers strive to optimize (among other things):**
  – Size, Weight, Power …
  – Selected parts from approved lists to minimize logistics tail
  – Technologically advanced parts to meet the “requirement” for the new system

• **What do you do if every part may someday be suspect?**
Engineering Challenges
(brought on by counterfeits)

• Different forms of counterfeit and fraudulent parts carry different reliability and performance curves.

• However, designing a system to be tolerant of counterfeits (if they get through the screening processes) is the biggest challenge engineers will face!
GIDEP Reporting  
(Information Sharing Portal)

• Most companies and agencies have some sort of “Quality Deficiency Reporting System”

• GIDEP is a way of linking the knowledge in these systems together for the “collective good”

• Mandatory reporting of non-conformances (including suspected or confirmed counterfeits)

• Coordination between GIDEP* and PDREP**

• Modernize GIDEP system (entry; storage; retrieval)

• Efficient correlation of specific issues to specific applications

* Government-Industry Data Exchange Program
** Product Deficiency Reporting and Evaluation Program
How Industry Can Help

• **Tighten up your supply chain**
  – Establish benchmarks for good suppliers
  – Adopt / identify good non-government standards

• **Help us and each other by reporting Major and Critical Non-conformances, of which counterfeits is a subset**

• **“Design in” protection against counterfeits**
How Industry Can Help
(from morning agenda)

- Standards
- Identification
- Risk Assessment
- Avoidance Protocols
- Test Methodologies
- Compliance
Systems Engineering: Critical to Program Success

Innovation, Speed, and Agility

http://www.acq.osd.mil/se