



# New DoD Protections Against Counterfeit Parts: Is Your Company Ready?

Richard Arnholt  
Grant Book  
Addie Cliffe

Richard Arnholt  
rarnholt@crowell.com  
202.624.2792

Grant Book  
gbook@crowell.com  
202.624.2512

Addie Cliffe  
acliffe@crowell.com  
202.624.2816

# Overview



- Background on counterfeit parts in the Department of Defense (“DoD”) supply chain
- Current environment: congressional response and DoD guidance
- Looking forward: what to expect and practical pointers for risk-mitigation

# DoD susceptibility to counterfeit parts



- Factors include:
  - U.S. defense systems increasingly dependent on electronic parts
  - Component obsolescence
  - Sophistication of counterfeiters
  - Certain countries openly allow counterfeiting (e.g., China)

# Congressional Investigation



- In 2011, the Senate Armed Services Committee (“SASC”) initiated an investigation into counterfeit electronic parts in the DoD supply chain
- Investigation in response to concerns about the performance and reliability of small, sophisticated electronic components relied on for national security and the protection of military personnel
- Report came out on May 21, 2012

# SASC Report: Key Findings



- Prevalence of counterfeit parts in the DoD supply chain
  - Over a two-year period, the investigation uncovered approximately 1,800 cases of suspect counterfeit electronic parts (looking at just part of the supply chain)
  - Total number of individual suspect parts exceeded one million

# SASC Report: Key Findings



- Suppliers of counterfeit goods
  - Of the 100 cases that SASC was able to track, the vast majority (70%) led to China
  - SASC concluded that China is the “epicenter of the global trade in counterfeits”
  - Canada and the UK were also significant sources, but SASC indicated that these countries were merely resale points for suspect parts from China

# SASC Report: Key Findings



- Counterfeit parts drive up defense costs
  - Immediate costs of replacing counterfeit parts and taking any necessary corrective action
  - Additional cost of long-term reliability problems
  - According to a DoD official:
    - “Unreliable systems have higher sustainment costs because, quite plainly, they break more frequently than planned. . . . Poor reliability leads to higher sustainment cost for replacement spares, maintenance, repair parts, facilities, staff, etc.”

# SASC Report: Key Findings



- Spotty reporting by contractors
  - SASC was critical of industry for untimely, inconsistent, and incomplete reporting
  - SASC noted that many cases go unreported to the Government-Industry Data Exchange Program (“GIDEP”)
    - Only 271 reports submitted to GIDEP during 2009 and 2010



# SASC's Areas of Concern



- DoD not well informed of the scope and impact of counterfeit parts in its systems
- Contractors not encouraged to adopt aggressive counterfeit avoidance and detection programs if they are able to recover costs incurred as a result of their own failure to initially detect counterfeit parts
- Defense industry's reliance on independent distributors to procure electronic parts for critical military systems "results in unacceptable risk"
- Weak testing regime for electronic parts exploited by counterfeiters

# Congressional Response



- FY2012 and FY 2013 National Defense Authorization Acts (“NDAAs”) include provisions to address the weaknesses identified by SASC
- FY2012NDAA, Section 818 requires DoD to promulgate regulations to implement a risk-based approach to minimize the impact of counterfeit or suspect counterfeit electronic parts



- “Covered” contractors
  - Contractors that perform work for DoD under Cost Account Standards (“CAS”) covered contracts
  - “covered” entities must flow down the Section 818 obligations to their subcontractors, vendors, and suppliers



- Covered contractors that supply electronic parts – or products that include electronic parts – are responsible for:
  - Detecting and avoiding the use or inclusion of counterfeit parts or suspect counterfeit parts in such products; and
  - The cost of any remedial rework or corrective action required due to the use of such parts
    - Open question – will liability for costs for rework or corrective action apply only to parts delivered after the law’s effective date, or to whatever parts may be in DoD’s inventory and use?



- Obtain parts from **original manufacturers** whenever possible: contractors and subcontractor at all tiers will be required to:
  - Obtain electronic parts that are **in production or in stock** from the OEM, the manufacturer’s authorized dealers, or “trusted suppliers” who obtain parts from the original manufacturers or their authorized dealers; and
  - Obtain electronic parts that are **not in production** or currently available in stock from “trusted suppliers.”



- Establishment of policies and procedures
  - DoD contractors will need to establish policies and procedures “to eliminate” counterfeit parts from the supply chain
- Reporting by contractors
  - Required to report within 60 days when contractors become aware or have “reason to suspect” that any component or material contains counterfeit electronic parts or “suspect” counterfeit electronic parts, in writing and on GIDEP or similar system



- Immunity for reporting
  - Contractors not subject to civil liability when providing a report under Section 818, provided the contractor made a “reasonable effort” to determine whether the material concerned contained counterfeit electronic parts
- Sanctions
  - Section 818(h) adds a criminal offense for intentionally trafficking in military goods or services known to be counterfeit where the use, malfunction or failure is likely to cause serious injury or death, impairment of combat operations, or other “significant harm” to national security



- Deployment of unique identifiers (Section 807)
  - Item-unique marking methodologies on electronic parts
- A “Safe harbor” for contractors (Section 833)
  - Limited safe harbor which makes allowable the costs of replacing counterfeit parts and required remediation if:
    - Contractor has operational system to detect and avoid counterfeit parts that DoD reviewed and approved;
    - The parts in question had been “provided to the contractor as Government property”; and
    - The contractor was timely in reporting.





- DoD regulations implementing Section 818 of the 2012 NDAA, to be implemented through DFARS 2012-D-055 Parts 201, 232,244, were due September 26, 2012
- No organized, formal, or open process for public input or guidance as to whether the rule would be issued as proposed rule or interim, but immediately effective, rule
- In the meantime, a March 16, 2012 DoD memorandum, “Overarching DoD Counterfeit Prevention Guidance,” provided insight



- Defines counterfeit material as “an item that is an unauthorized copy or substitute that has been identified, marked, and/or altered already by a source other than the item’s legally authorized source and has been misrepresented to be an authorized item of the legally authorized source”
- Representing a used item as a new item can result in fraud charges
- Particular focus on mission critical components, critical safety items, electronic parts, and load-bearing mechanical parts

# DoD Guidance: Immediate Actions



- Investigate suspected counterfeit incidents and report confirmed counterfeits to “appropriate criminal authorities”
- Conduct Department-level review to identify “appropriate industry standards” to be used in contracting requirements
- Establish testing and verification requirements to apply to prime contractors, subcontractors and suppliers, with respect to items not received from OEMs, OCMs, or authorized distributors, if the items are identified as having high risk for counterfeit potential

# DoD Guidance: Immediate Actions



- Report suspect or confirmed counterfeit items on GIDEP and ensure contractors and subcontractors report as well
- Require inclusion of DFARS clause 252.246-7003, “Notification of Potential Safety Issues,” in contracts for acquisition of specified items



- On April 26, 2013, the Under Secretary of Defense for Acquisition, Technology, and Logistics issued DoD Instruction No. 4140.67 to further establish policy to prevent counterfeit material at any level of the DoD supply chain.
- Instruction serves to (1) establish DoD's policies and (2) assign responsibility for the prevention, detection, and remediation of counterfeit material.

# DoD Instruction - Policy



- Employ a “risk-based” approach
- Reduce frequency and impact of counterfeit material by applying prevention and early detection procedures within the supply chain
- Strengthen oversight and surveillance procedures for critical material
- Investigate all cases of suspected counterfeit material
- Document all occurrences of suspected and confirmed counterfeit material



- Make information about counterfeiting available at all levels of the supply chain
- Seek restitution when cases of counterfeiting are confirmed
- Notify criminal investigative organizations or intelligence authorities and those who use such materials at earliest opportunity

# DoD Instruction – Responsibility



- DoD component heads responsible for integrating anti-counterfeiting policy into all relevant contract requirements
- DoD component heads must procure material from suppliers that meet appropriate counterfeit avoidance criteria or apply additional counterfeit risk management measures when such suppliers are not available



# Proposed DoD Regulations



- On May 16, 2013, DoD published proposed regulations partially implementing Section 818.
- Primary Components:
  - Definitions of key terms
  - Costs of remediating/replacing counterfeit parts unallowable (with very limited exception)
  - Purchasing system requirements to avoid and detect counterfeit parts
  - Withholds for deficient systems



### Counterfeit Part

- (1) An unauthorized copy or substitute part that has been identified, marked, and/or altered by a source other than the part's legally authorized source;
- (2) An item misrepresented to be an authorized item of the legally authorized source; or
- (3) A new, used, outdated, or expired item from a legally authorized source that is misrepresented by any source to the end-user as meeting the performance requirements for the intended use.



### **Legally Authorized Source**

The current design activity or the original manufacturer or supplier authorized by the current design activity or the original manufacturer to produce an item.

### **Suspect Counterfeit Part**

A part for which visual inspection, testing, or other information provide reason to believe that a part may be a counterfeit part.

# Proposed DoD Regulations

## – Cost Principles



- Contractors that are subject to Cost Accounting Standards that supply electronic parts under CAS-covered contracts are responsible for detecting and avoiding the use or inclusion of counterfeit electronic parts or suspect counterfeit electronic parts

# Proposed DoD Regulations

## – Cost Principles



- The costs of counterfeit or suspect counterfeit electronic parts and the cost to rework or remedy the use or inclusion of such parts is **expressly unallowable** unless:
  - The contractor has an operational system to detect and avoid such parts that has been reviewed and approved by DoD;
  - The parts are government-furnished property; **and**
  - The contractor provides timely notice.

# Proposed DoD Regulations

## – Purchasing System Requirements



- Amends DFARS 252.244-7001
- (c)(19) Establish and maintain policies and procedures to ensure purchase orders and subcontracts contain mandatory and applicable flowdown clauses . . . and any clauses required to carry out the requirements of the prime contract, **including the requirements of 252.246-70XX, Contractor Counterfeit Electronic Part Avoidance and Detection System, if applicable.**

# Proposed DoD Regulations

## – Purchasing System Requirements



- (c)(20) Provide for an organizational and administrative structure that ensure effective and efficient procurement of required quality materials and parts at the best value from responsible and reliable sources, **including the requirements of 252.246-70XX, Contractor Counterfeit Electronic Part Avoidance and Detection System, if applicable.**

# Proposed DoD Regulations

## – Purchasing System Requirements



- Creates DFARS 252.246-70XX, Contractor Counterfeit Electronic Part Avoidance and Detection System
- The contents of this clause are copied directly from the nine elements contained in Section 818



# Proposed DoD Regulations

## – Purchasing System Requirements



- System shall address:
  - Training of personnel;
  - Inspection and testing of electronic parts;
  - Processes to abolish counterfeit parts proliferation;
  - Mechanisms to enable traceability of parts to suppliers;
  - Use and qualification of trusted suppliers;
  - Reporting and quarantining of counterfeit and suspect counterfeit electronic parts;
  - Methodologies to identify suspect counterfeit parts and determine if, in fact, counterfeit;
  - Design, operation, and maintenance of systems to detect and avoid such parts; and
  - Flow down of avoidance and detection requirements to subcontractors.

# Industry Response



- Not well received
- The proposed rule long overdue and only partially implements Section 818
  - Significant components of what will comprise an “acceptable” system, such as trusted supplier and reporting requirements wholly unaddressed
  - Difficult to provide meaningful comments without coordinated understanding of how DoD intends to implement all aspects of Section 818
- Inconsistent with other guidance and instructions
  - Digresses from risk-based approach described in DoD Instruction and mandated by Section 818
  - Definitional inconsistencies

# Industry Response

## – Small Business



- Proposed rule states will only affect large contractors subject to CAS
- However, because covered contractors are required to flow down the counterfeit avoidance and detection requirements to subcontractors at every tier, it is likely that small business will be affected
- Costs to establish such systems could have disproportionate impact on small business, which may not be able to absorb the cost impact
- If every purchase order presents potential for significant liability, small businesses may exit the DoD supply chain altogether, making it difficult for prime contractors and the government to meet small business targets

# Industry Response – Definitions



- Counterfeit Part
  - Omits any element of intent to mislead, defraud or deceive
  - Treats as counterfeit genuine parts that are out of spec or suffer quality issues
  - Does not conform to DoD Instruction 4140.67 or industry standards

# Industry Response

## – Cost Principles



- “Expressly” Unallowable
  - Expressly is a term of art that introduces penalties and is beyond requirements of Section 818
- Too broad of cost exclusion for any reworking required due to counterfeit part
- Because change is implemented through purchasing system, would likely apply beyond CAS-covered contracts as contractors are not likely to have separate purchasing systems
- Unclear Safe Harbor Provision, which appears to apply only if government furnished property

# Structural Challenges



- DoD systems with long life cycles are reliant on commercial electronic parts with short life cycles
  - Obsolete parts aren't available from OEM's
  - DoD demand insufficient to warrant continued production
  - Electronic components manufactured in unsecure locations
- Tension between drive to secure the supply chain (higher costs) and fiscal constraints
- Move away from reliance on commercial supply chain?

# What Should Contractors Do?



- Prior to finalization of DoD regulations, contractors can take proactive steps to reduce exposure:
  - Comprehensive self-examination to assess scope and nature of exposure to counterfeit electronic parts
  - Re-examination of supplier policies
  - Reporting of counterfeit parts
  - Flow-down of liability for counterfeit parts and reporting requirements to subcontractors and suppliers
  - Consider price impact

# Practical Pointers



- Steps to take to minimize risk of allowing counterfeit parts to enter the DoD supply chain:
  - Review and revise policies, procedures, and/or methodologies regarding supply chain risk
  - Personnel training





- Protocols:
  - For investigation of suppliers and parts
  - For testing and inspection
  - For quarantining parts
  - For remediation, including segregation of associated costs
  - For notification to customers (DoD components or higher-tier contractors)

# Practical Pointers

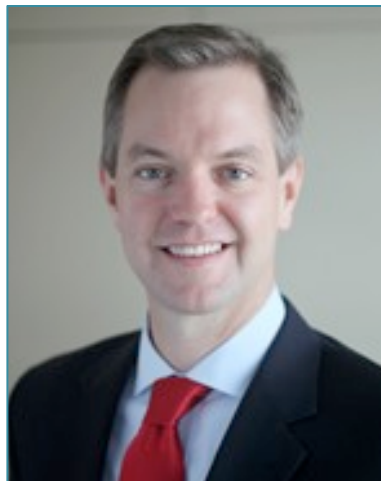


- Development of trusted suppliers
- Flowing down necessary requirements to subcontractors, suppliers, and vendors
- Testing and monitoring compliance by subcontractors, suppliers and vendors



# Questions / Comments / Feedback / Discussion

# Contact Us



Richard Arnholt



Grant Book



Addie Cliffe