

# The New DoD Rules on Counterfeit Electronic Parts

Chris Haile

Cathy Kunz

Richard Arnholt

Grant Book

Jason Lynch

June 5, 2014

# Introductions



Chris Haile



Cathy Kunz



Richard Arnholt



Grant Book



Jason Lynch

# Agenda

- Context of the New Rule
  - Basis of Concern
  - Congressional Action
  - Rulemaking
- General Scope of the Rule and Key Definitions
- Detection and Avoidance System Requirements
- Reporting Suspect Counterfeit Parts
- Audits of Systems
- Cost Allowability Rules
- Implementation and Challenges

# Context of the New Rule

# 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 (“NDAAAs”) include provisions to address the weaknesses identified by SASC
- FY2012 NDAA, Section 818 requires DoD to promulgate regulations to implement a risk-based approach to minimize the impact of counterfeit or suspect counterfeit electronic parts

# FY2012 NDAA

- “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

# FY2012 NDAA

- 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

# FY2012 NDAA

- 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."

# FY2012 NDAA

- 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

# FY2012 NDAA

- 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

# FY2013 NDAA

- 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

- DoD plans to release regulations in three parts
- First part, released May 16, 2013 as a proposed rule, and May 6, 2014 as a final rule, provides foundation for detection and avoidance of counterfeit parts
- Second part, released December 3, 2013 as a proposed rule, amends the regulations regarding the use of higher-level quality systems (such as ISO, ASQ, and SAE standards)
- Third part, not yet released, should address the reporting requirements for identified counterfeit parts

# DoD Regulations – Part 1

- Supposed to lay the foundation
- 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

## DoD Regulations – Part 2

- By its own admission, “does not directly implement any specific aspect of section 818”
- Instead, it continues DoD’s focus on contractor’s purchasing systems to stem the impact of counterfeit parts by amending the regulations regarding the use of higher-level quality systems
- Its stated purpose is “to ensure that agencies assess the risk of nonconforming items when determining whether higher-level quality standards should be used by the Government and relied on by contractors”

# DoD Regulations – Part 2, cont.

- Revises FAR 44.303 to add implementation of higher-level quality standards to areas for evaluation when conducting a review of a contractor's purchasing system
- Makes small changes to FAR 46.202-4, which addresses higher-level quality systems
  - Adds “design” and “testing” to the list of examples of technical requirements requiring control
  - Revises quality standards to remove outdated or obsolete standards as well as including higher-level quality standards related to counterfeit electronic parts and materials
- Sets selection of the appropriate standard with the contracting officer by revising FAR 46.311 to clarify that if the clause is used, the contracting officer is required to list one or more higher-level quality standard and revising FAR 52.246-11 to remove the opportunity for the offeror to select the standard

# Scope of the New Rule

# Summary of Scope

- If the contractor is covered, it must implement a “counterfeit electronic part detection and avoidance system” that complies with the new rule.
- What contracts are covered?
  - Subject to Cost Accounting Standards (CAS)
  - And that supply:
    - Electronic parts
    - End items, components, parts or assemblies containing electronic parts, or
    - Services where any of the above are provided as part of the service

# Flowdown

- Not only CAS-covered primes, but all subcontractors providing electronic parts
  - Including commercial, COTS
- Flow-down is part of purchasing system
  - DFARS § 246.870-2(b)(9)
- May affect parts already in the contractor's possession (“on the shelf”)

# Key Definitions

# New Definitions

- “Electronic Part”

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.

# “Counterfeit [Electronic] Part”

## Proposed:

- (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 and has been misrepresented to be from a 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.

## Final:

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.

# Dropped Definition

- “Legally authorized source”
  - DoD revised the definition of Counterfeit Electronic Part “to list the sources legally authorized to permit manufacturing or resale of the item.”
  - I.e., “legally authorized source” now subsumed by “counterfeit electronic part.”

# “Counterfeit Electronic Part” Flowchart

- (1) An unlawful or unauthorized
  - reproduction,
  - substitution, or
  - alteration
- (2) That has been knowingly:
  - mismarked,
  - misidentified, or
  - otherwise misrepresented
- (3) 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.

# “Suspect Counterfeit Electronic Part”

## Proposed:

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

## Final:

“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.”

# Other Terms

- “Obsolete Electronic Part” Added
  - “An electronic part that is no longer in production by the original manufacturer or an aftermarket manufacturer that has been provided express written authorization from the current design activity or original manufacturer.”
- “Trusted Supplier” Undefined
  - NDAA § (c)(3)
  - 19 commenters asked for a definition
  - “DoD is concerned that defining and using the term ‘trusted supplier’ would create confusion.”
  - The systems criteria “are revised to express what is intended by ‘trusted supplier’ without directly using the term.”
    - E.g., “suppliers that meet applicable counterfeit detection and avoidance system criteria.”

# System Requirements & Reporting

# What is Required?

System must include risk-based policies and procedures that address 12 criteria

1. Training of personnel
2. Inspection and testing of electronic parts, including criteria for acceptance and rejection
3. Process to abolish counterfeit parts proliferation
4. Process for maintaining electronic part traceability

# System Criteria 5-8

5. Use of suppliers that are original manufacturer, sources with the express written authority of the original manufacturer or the current design activity, including an authorized aftermarket manufacturer or supplier that obtains parts exclusively from one or more of these sources
6. The reporting and quarantining of counterfeit and suspect counterfeit electronic parts
7. Methodologies to identify suspect counterfeit electronic parts and to rapidly determine if a suspect counterfeit electronic part is, in fact, counterfeit
8. Design, operation, and maintenance of systems to detect and avoid counterfeit electronic parts and suspect counterfeit electronic parts

# System Criteria 9-12

9. Flow-down of counterfeit parts detection and avoidance requirements to subcontractors and suppliers
10. Processes for keeping continually informed of current counterfeiting information and trends
11. Process for screening the Government-Industry Data Exchange Program (GIDEP) reports and other credible sources of counterfeiting information
12. Control of obsolete electronic parts

# Concerns about Criteria

- Criteria do not address structural problems
  - Obsolescence, global supply chain, commercial item
- Dealing with mods adding these requirements
  - Primes - Costs of mitigating counterfeit parts may not be allowable, but costs to implement these new systems are
  - Subcontractors – possible basis for price adjustment

# Audit of Systems/Cost Allowability Rule

# New DFARS Cost Rule

- DFARS 231.205-71
  - makes the costs of counterfeit electronic parts or suspect counterfeit electronic parts and the cost of rework or corrective action that may be required to remedy the use or inclusion of such parts unallowable.
  - Narrow exception: (1) the contractor has a reviewed and DOD-approved operational system to detect and avoid counterfeit parts and suspect counterfeit electronic parts; (2) the counterfeit electronic parts or suspect counterfeit electronic parts are government-furnished property; and (3) the contractor provides timely (i.e. within 60 days after becoming aware) notice to the government.

# Contractor Purchasing System Review

- Contractors' counterfeit electronic parts detection and avoidance system will now be reviewed during a Contractor Purchasing System Review performed by DCMA.
- The review will include an examination of the contractor's policies and procedures related to the detection and avoidance of counterfeit electronic parts.
- If a deficiency related to the counterfeit electronic parts detection and avoidance system is determined by the ACO to be significant, the purchasing system may be disapproved and a withholding of payments can result.

# Contractor Purchasing System Review

- Rule established two versions of the Contractor Purchasing System Administration clause, DFARS 252.244-7001.
  - “Basic” clause is supplemented to add additional criteria to subsection (c) (that identifies the attributes a contractor’s purchasing system must have) related to a counterfeit electronic parts detection and avoidance system, and the “Basic” clause will be included in solicitations and contracts that contain FAR 52.244-2, Subcontracts.
  - “Alternate I” clause contains only the criteria related to a counterfeit electronic parts detection and avoidance system in subsection (c) and will be included in solicitations and contracts where compliance with the new DFARS 252.246-7007, Contractor Counterfeit Electronic Part Detection and Avoidance System, is required but otherwise do not contain FAR 52.244-2, Subcontracts.

# Contractor Purchasing System Review

- DCMA has indicated it plans to issue “Counterfeit Detection and Avoidance System Checklist” concerning its review of contractors’ counterfeit electronic parts detection and avoidance system .
  - It is unclear how DCMA will review a contractors’ counterfeit electronic parts detection and avoidance system until such guidance is issued.
- DCMA’s guidance for conduct of Contractor Purchasing System Review is available at [dcma.mil](http://dcma.mil)

# Implementation and Challenges

# Challenges for Implementation

- Flowdown challenges
- Impacts on commercial and mixed supply chains
- Undefined standards and risk-based concepts
- Government audits
- Monitoring compliance and determining when to report
- Impacts on existing inventories

# What Should Contractors Do Now?

- If you have the clause, then you must have a system
- Comprehensive self-examination to assess scope and nature of exposure to counterfeit electronic parts
- Re-examination of supplier policies, procedures and methodologies regarding supply chain risk
- Personnel training
- Flow-down of liability for counterfeit parts and reporting requirements to subcontractors and suppliers
- Develop “trusted suppliers”
- Testing and monitoring compliance by subcontractors, suppliers and vendors pursuant to system
- Consider price impacts

# Protocols

- Investigation of suppliers and parts
- Testing and inspection
- Quarantining parts
- Remediation, including segregation of associated costs
- Notification (GIDEP, DoD components, higher-tier contractors, mandatory disclosure)
- Following GIDEP reports
- Maintaining currency to industry standards

# Conclusion

# Contacts

Chris Haile

[chaile@crowell.com](mailto:chaile@crowell.com)

202-624-2898

Catherine Kunz

[ckunz@crowell.com](mailto:ckunz@crowell.com)

202-624-2957

Richard Arnholt

[rarnholt@crowell.com](mailto:rarnholt@crowell.com)

202-624-2792

Grant Book

[gbook@crowell.com](mailto:gbook@crowell.com)

202-624-2512

Jason Lynch

[jlynch@crowell.com](mailto:jlynch@crowell.com)

202-624-2678