

Hidden Risks in the Supply Chain

Steve McNamara
September 9, 2015

What You Can't See Can Hurt You

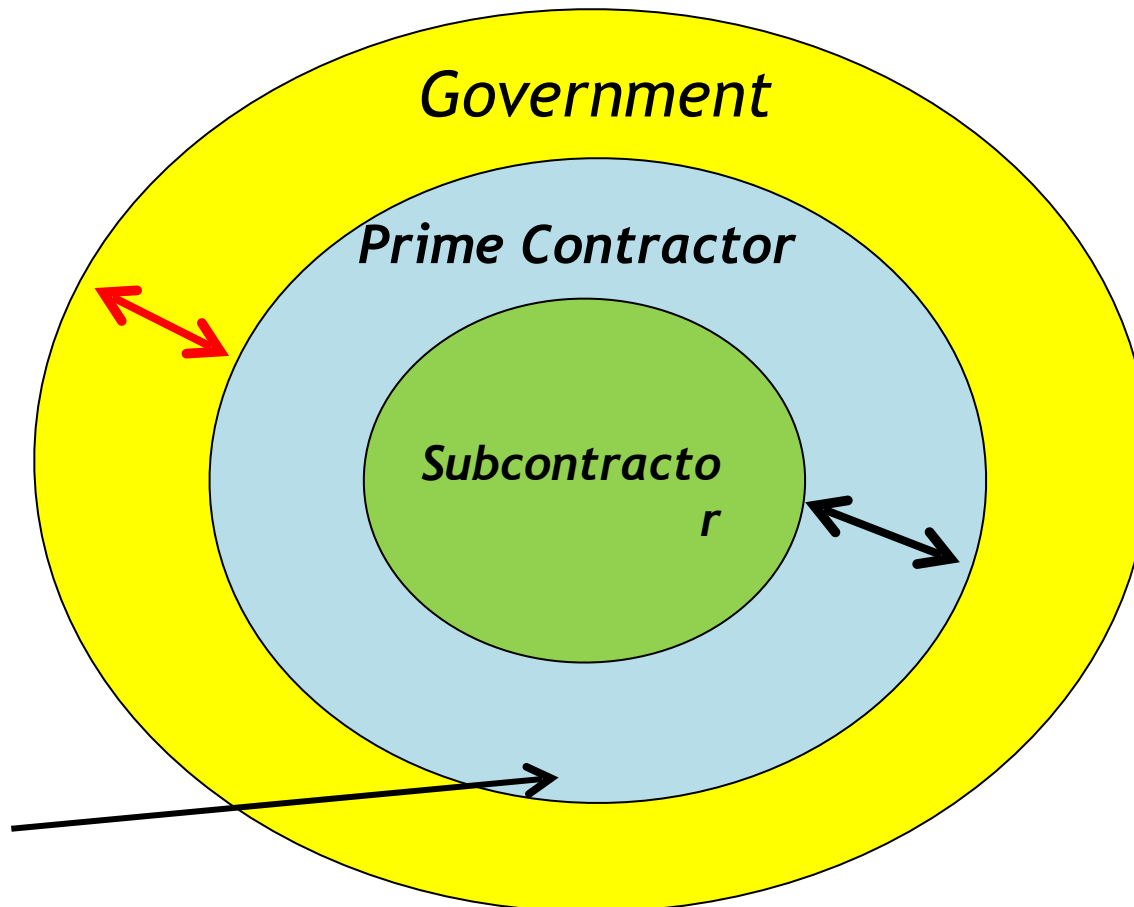
- *No Privity of Contract with Lower-tier Suppliers*
- *Terms and Conditions*
- *Counterfeit Parts*
- *Escape Defects*
- *Unqualified Suppliers*
- *Lack of Visibility*
- *Poor Source Selection*



Privity of Contract

Privity Between Government and Prime 

Privity Between Prime and Subcontractor 

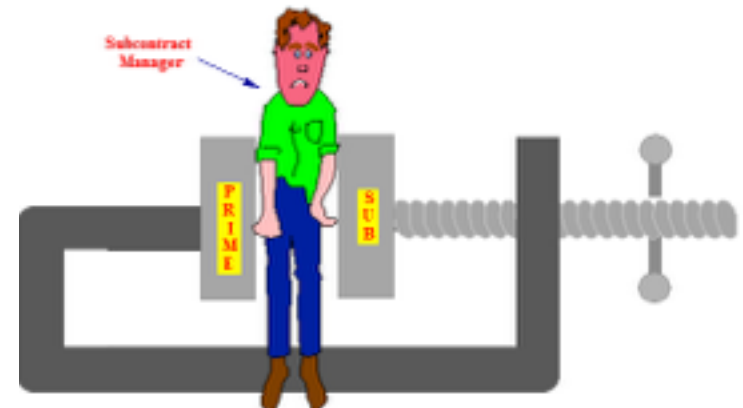


No Privity exists
between
Government and
Subcontractor

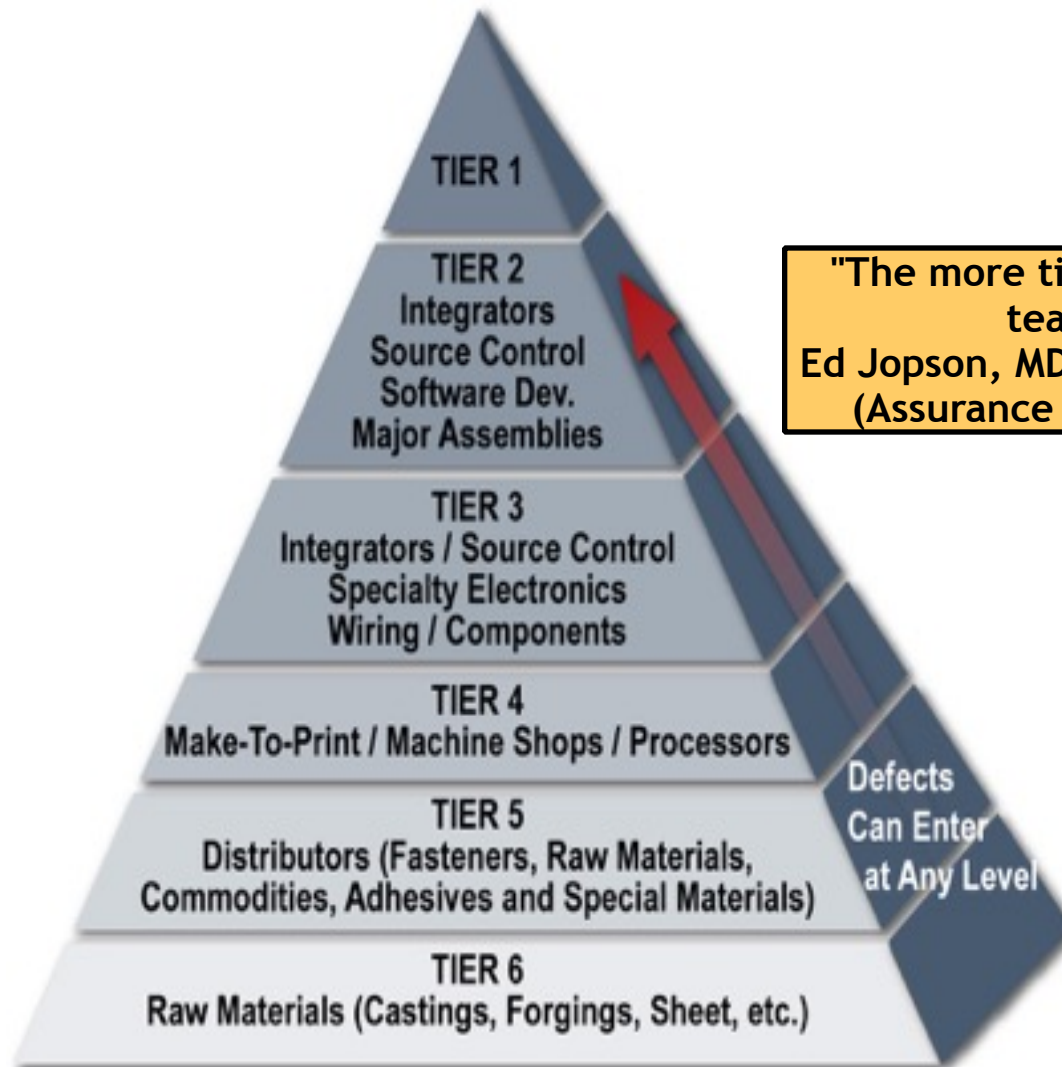
Incompatible Terms and Conditions

Areas of vulnerability:

- Specifications
- Contractual Terms and Conditions
- Payment Terms
- Funding
- Warranties
- Rights in data and data access
- Termination clauses
- Post delivery support
- Access to facilities
- Schedules



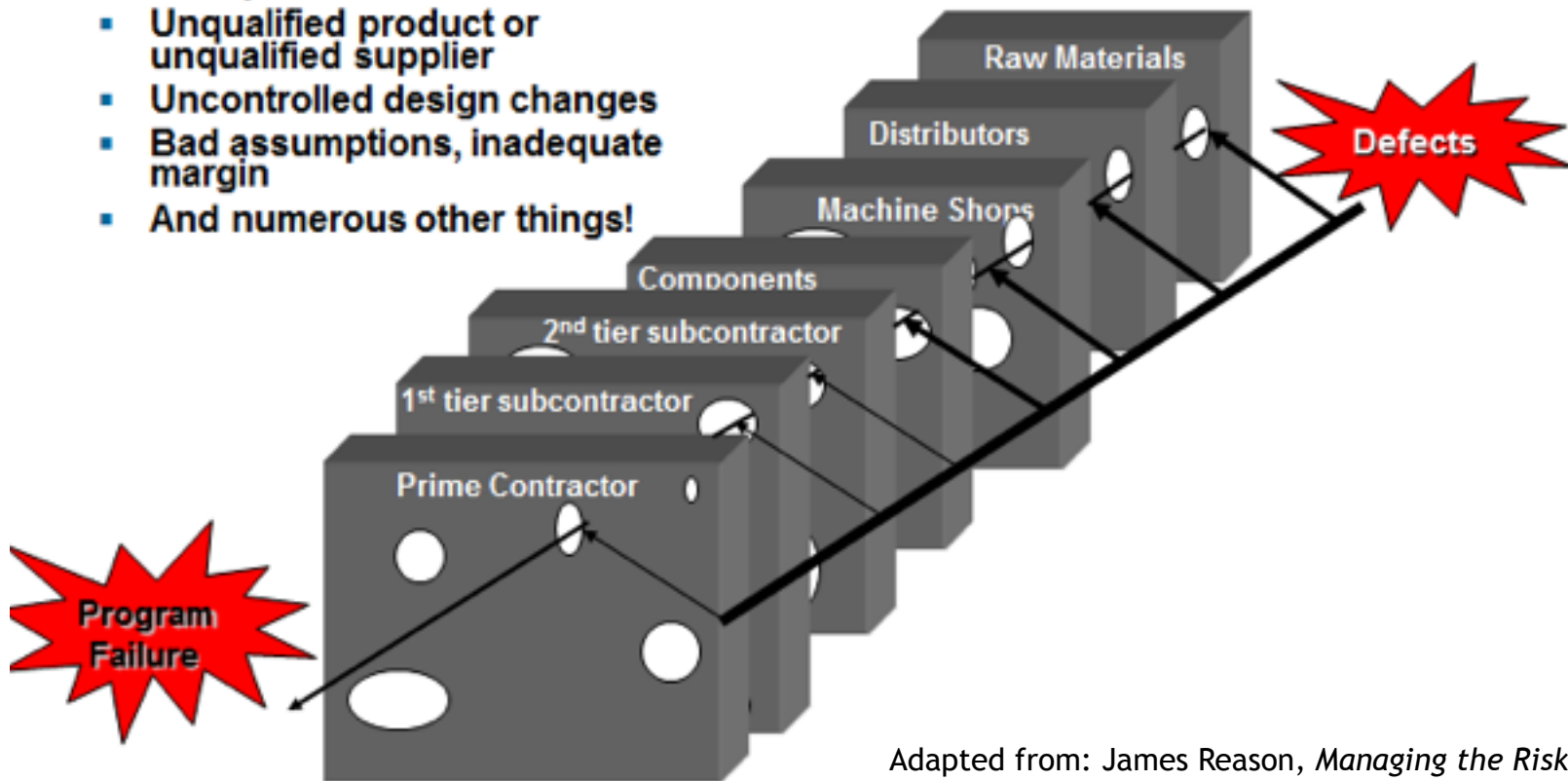
Lower-tier Supplier Management



Defects In The Supply Chain Can Be Devastating

Failures can be the result of:

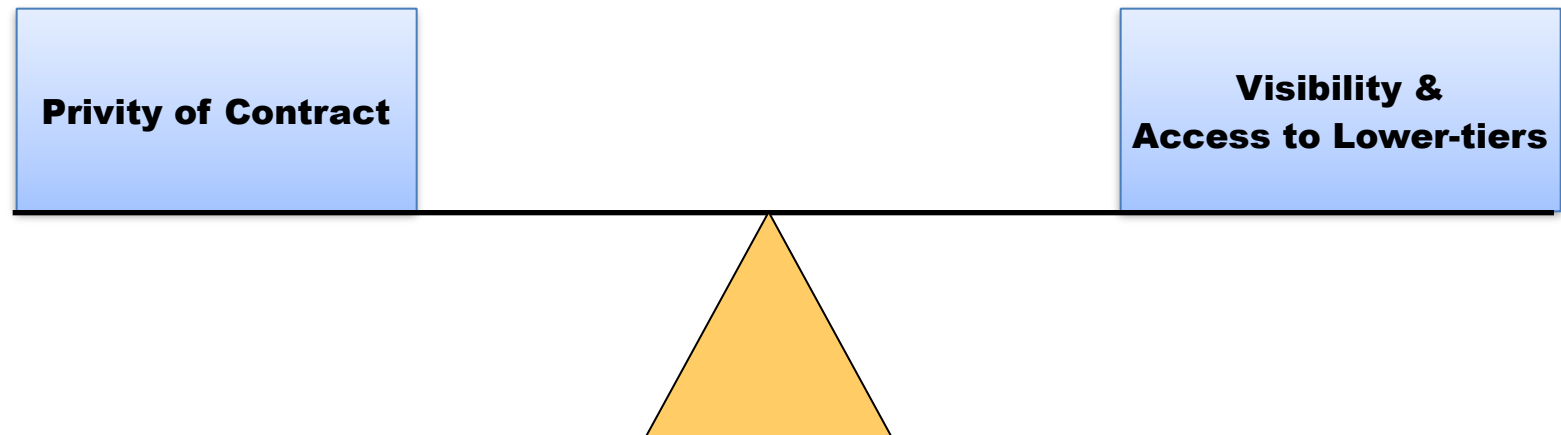
- Inadequate requirements flow-down
- Poor process control
- Unqualified product or unqualified supplier
- Uncontrolled design changes
- Bad assumptions, inadequate margin
- And numerous other things!



Adapted from: James Reason, *Managing the Risks of Organizational Accidents*, 1997, p. 12

Balancing Lower-Tier Supplier Management

- How do we apply to lowest levels of the Supply Chain?
- How do we ensure our contractual rights to audit?
- How do we validate processes within the Supply Chain?
- How do we ensure that the lower-level suppliers manage their supply chain?



Demand Supplier Management of Next Lower Tier Supplier (LTS)



- Step 1 - Define expectations
 - Focus capture and evaluation processes to include lower tier management
 - Flow down requirements - including quality clauses, technical specification allocation, linked and integrated schedules, terms and conditions (sub-tier access), risk assessment, mandatory pass-thru to sub-tier suppliers
 - Identify high risk suppliers and mitigate risk
- Step 2 - Source evaluation and selection - add criteria:
 - Thoroughness of higher risk supplier identification
 - Quantity and experience of resources to manage LTS
 - Risk mitigation plans
 - Flow down of management provisions to LTS
 - Program performance - focus on risk associated with LTS

Demand Supplier Management of Next Lower Tier Supplier (LTS)



- Step 3 - Improve proactive management
 - Subcontract Management Teams implementing improved insight/oversight
 - Increased QA/MA participation
 - Plan for lower tier management in program funding
 - Focus on supplier process adherence at all tiers
 - Add sub-tier management throughout process: instructions in RFP
 - Require 1st tier suppliers to:
 - Identify higher risk sub-tier suppliers in the risk management plan,
 - Tailored risk assessment for small suppliers
 - Provide visibility to sub-tier supplier performance

Indicators of Effective Lower-tier Processes



- How does the lower-tier supplier manage and control its suppliers?
 - Source Selection
 - Requirements Flow-down
 - Quality (pre-award surveys, audits, corrective actions)
 - Special Processes
- Look for evidence of effective and strong processes in the Suppliers' Supply Chain Management infrastructure
 - Review their internal procedures
 - Look at some Subcontracts and Purchase Orders
 - Review their Quality Records
 - Review special process controls
 - How frequently do they audit their suppliers?
 - Sample some failure analyses, root cause, and corrective actions
 - Meet with their supplier management and quality personnel

Rating Suppliers

- Rating systems should have the following attributes:
 - Frequent
 - Objective
 - Consistent across the enterprise
 - Ability to rate Lower-tier Supplier Management
 - Ability to rate Hardware, Software and Services Suppliers
 - 360° feedback to suppliers
 - Management review
 - Supportive of analysis

Sample Supplier Rating

1 Basic Information		2 Scores / Comments		3 Upload Documents		4 Summary	
Supplier: American Gage, Placentia, CA (ERP: 103096) Subcontract / PO #: SB421567 Subcontract / PO # Description: N/A		Program: Drone Status: In Evaluation Phase		Effective Date: 3/31/2015 Average Score:			
Category	Assessment Comments		Internal Comments				
Management							
Management Responsiveness	<input type="radio"/> N/A <input checked="" type="radio"/> 1 <input type="radio"/> 2 <input type="radio"/> 3 <input type="radio"/> 4		Always responsive to customer concerns				
Program Management	<input type="radio"/> N/A <input checked="" type="radio"/> 1 <input type="radio"/> 2 <input type="radio"/> 3 <input type="radio"/> 4		Provides outstanding program management support				
Risk and Opportunity Management	<input type="radio"/> N/A <input checked="" type="radio"/> 1 <input type="radio"/> 2 <input type="radio"/> 3 <input type="radio"/> 4		Plan is missing some critical areas				
Process Improvement	<input checked="" type="radio"/> N/A <input type="radio"/> 1 <input type="radio"/> 2 <input type="radio"/> 3 <input type="radio"/> 4						
Staffing	<input type="radio"/> N/A <input checked="" type="radio"/> 1 <input type="radio"/> 2 <input type="radio"/> 3 <input type="radio"/> 4		Meeting required staffing profile				
General Management	<input type="radio"/> N/A <input checked="" type="radio"/> 1 <input type="radio"/> 2 <input type="radio"/> 3 <input type="radio"/> 4		Generally acceptable				
Technical							
Product Performance	<input type="radio"/> N/A <input checked="" type="radio"/> 1 <input type="radio"/> 2 <input type="radio"/> 3 <input type="radio"/> 4		Meets all requirements and exceeds some key performance parameters				
Systems Engineering	<input type="radio"/> N/A <input checked="" type="radio"/> 1 <input type="radio"/> 2 <input type="radio"/> 3 <input type="radio"/> 4		Highly effective system engineering processes in place				
Software Engineering	<input checked="" type="radio"/> N/A <input type="radio"/> 1 <input type="radio"/> 2 <input type="radio"/> 3 <input type="radio"/> 4						
Logistics and Sustainment	<input checked="" type="radio"/> N/A <input type="radio"/> 1 <input type="radio"/> 2 <input type="radio"/> 3 <input type="radio"/> 4						

Sample Supplier Rating

Schedule		
Schedule	<input type="radio"/> N/A <input checked="" type="radio"/> 1 <input type="radio"/> 2 <input type="radio"/> 3 <input type="radio"/> 4	Delivery rate 100.00 %
SPI	<input type="radio"/> N/A <input checked="" type="radio"/> 1 <input type="radio"/> 2 <input type="radio"/> 3 <input type="radio"/> 4	1.20
Cost		
Cost	<input checked="" type="radio"/> N/A <input type="radio"/> 1 <input type="radio"/> 2 <input type="radio"/> 3 <input type="radio"/> 4	
CPI	<input type="radio"/> N/A <input checked="" type="radio"/> 1 <input type="radio"/> 2 <input type="radio"/> 3 <input type="radio"/> 4	1.20
Financial Health		
	<input checked="" type="radio"/> N/A <input type="radio"/> 1 <input type="radio"/> 2 <input type="radio"/> 3 <input type="radio"/> 4	
Quality & Mission Assurance		
Quality	<input type="radio"/> N/A <input checked="" type="radio"/> 1 <input type="radio"/> 2 <input type="radio"/> 3 <input type="radio"/> 4	Acceptance rate 87.50 %
Process Effectiveness	<input checked="" type="radio"/> N/A <input type="radio"/> 1 <input type="radio"/> 2 <input type="radio"/> 3 <input type="radio"/> 4	
Supply Chain Management		
Supply Chain Management	<input checked="" type="radio"/> N/A <input type="radio"/> 1 <input type="radio"/> 2 <input type="radio"/> 3 <input type="radio"/> 4	
Customer Satisfaction		
Customer Satisfaction	<input checked="" type="radio"/> N/A <input type="radio"/> 1 <input type="radio"/> 2 <input type="radio"/> 3 <input type="radio"/> 4	
Assessment Summary		
Provides outstanding program management support		
Evaluation Scale		
■ Definite Problem	Subcontractor performance has definite problems. Critical issues require management attention above the project manager level for resolution.	
■ Potential Problem	Subcontractor performance has potential problems. Issues are being resolved with the attention of project management.	
■ As Planned	Subcontractor performance is as planned. Activities and results are as expected. No issues.	
■ Better than Planned	Supplier performance is significantly better than planned. Activities and results are significantly better than expected. No issues.	

Lower-tier Supplier Management

Counterfeit Parts

- Counterfeit parts have become an increasingly serious threat to the aerospace and defense industry
- Counterfeit electronic and mechanical parts have entered the supply chain primarily from 3rd world sources and China
 - Many of these parts have been salvaged from discarded computers and other waste products and then remarked and re-branded for sale by unscrupulous brokers



Much of the material used to make counterfeit electronic parts is electronic waste (e-waste) shipped from the U.S. and the rest of the world to China. In its January 2010 study, the Department of Commerce's said that e-waste has turned into an abundance of discrete electronic components and microcircuits for counterfeit parts. The failure of a single electronic part can leave a soldier, sailor, airman, or Marine vulnerable at the worst possible time. A flood of counterfeit electronic parts has made it a lot harder to have confidence that won't happen.

- Senator Carl Levin

The Problem With Electronic Waste

Electronic Waste → Components Removed → Sorted By Package/Lead Types



Counterfeit Parts

- The net result is that some of the most complex and sophisticated defense systems have been made vulnerable by the infiltration of counterfeit parts, placing our warfighters in harm's way and weakening the defense of our nation
- This threat became so serious that in 2012, the Senate Armed Services Committee held hearings on this subject
- The GAO issued a report in February 2012 stating that: *“Counterfeit parts - generally the misrepresentation of parts’ identity or pedigree - can seriously disrupt the Department of Defense (DOD) supply chain, harm weapon systems integrity, and endanger troops’ lives.”*
- The CEO’s from some of the top Defense Contractors were called before the Senate to testify on the impact of counterfeit parts on their programs
- As a result of these hearings the 2012 National Defense Authorization Act was amended to include Section 818 to provide strict preventive measures for counterfeit parts

Section 818 Summary

Section 818 of the 2012 NDAA, which is now the law, states that:

- Contractors who supply electronic parts or products that include electronic parts are responsible for detecting and avoiding the use or inclusion of counterfeit electronic parts or suspect counterfeit electronic parts in such products and for any rework or corrective action that may be required to remedy the use or inclusion of such parts
- The cost of counterfeit electronic parts and 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 are not allowable costs under Department of Defense contracts
- Any contractor or subcontractor who becomes aware, or has reason to suspect, that any end item, component, part, or material contained in supplies purchased by a contractor or subcontractor contains counterfeit electronic parts or suspect counterfeit electronic parts report in writing within 60 days to appropriate Government authorities and the Government-Industry Data Exchange Program

DFARS Case 2012-DO55 Final Ruling

May 6, 2014



- DoD reviewed the public comments in the development of the final rule. A Summary of Significant Changes From Proposed Rule is as follows:
 - The definitions of “counterfeit part” and “suspect counterfeit part” are substantively revised and limited to electronic parts;
 - The definition of “legally authorized source” is deleted; and
 - A new definition of “obsolete part” is added.
 - The criteria for a contractor's counterfeit electronic part detection and avoidance system at DFARS 246.870-2(b) and paragraph (c) of the clause at DFARS 252.246-7007 are expanded and clarified and three new criteria have been added. In addition, the use of a risk-based system by the contractor is clarified.
 - Applicability of the counterfeit system criteria only to CAS-covered prime contractors is clarified, as is the required flow down to all subcontractor tiers providing electronic parts or assemblies containing electronic parts.

Summary of DFARS 246.870-2(b)



- Contractors that are subject to the Cost Accounting Standards (CAS) and that supply electronic parts or products that include electronic parts and their subcontractors that supply electronic parts or products that include electronic parts, are required to establish and maintain an acceptable counterfeit electronic part detection and avoidance system. Failure to do so may result in disapproval of the purchasing system by the contracting officer and/or withholding of payments (see [252.244-7001](#), Contractor Purchasing System Administration).

Summary of 252.246-7007

- *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.
- The Contractor shall establish and maintain an acceptable counterfeit electronic part detection and avoidance system. Failure to maintain an acceptable counterfeit electronic part detection and avoidance system, as defined in this clause, may result in disapproval of the purchasing system by the Contracting Officer and/or withholding of payments.

Summary of 252.246-7007

Counterfeit electronic part detection and avoidance system shall include risk-based policies and procedures that address, at a minimum, the following areas:

- 1) The training of personnel
- 2) The inspection and testing of electronic parts
- 3) Processes to abolish counterfeit parts proliferation
- 4) Processes for maintaining electronic part
- 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.
- 7) Methodologies to identify suspect counterfeit parts and to rapidly determine if a suspect counterfeit part is, in fact, counterfeit.

Summary of 252.246-7007 (Continued)



- 8) Design, operation, and maintenance of systems to detect and avoid counterfeit electronic parts and suspect counterfeit electronic parts.
- 9) Flowdown 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.

Impact of DFARS Counterfeit Parts Clauses



- In order for your company to have an approved purchasing system, you must implement a counterfeit parts prevention program on all DoD programs subject to this new DFARS clause
- Contractors must purchase electronic parts or assemblies that contain electronic parts in accordance with the sourcing requirements of NDAA 2012 Section 818
 - Original Component Manufacturers or
 - Authorized Distributors
 - If parts are not available from the above, contractors must subject them to a rigorous inspection and testing protocol to validate authenticity
- Contractors must “establish and maintain an acceptable counterfeit electronic parts avoidance and detection system”. This is to be accomplished by flowing down “counterfeit system criteria” from the prime contractor to all subcontractor tiers providing electronic parts or assemblies containing electronic parts
- Contractors must report all instances when their program has reason to suspect that counterfeit parts have been used in deliverable products

AS5553A - The New Standard for Counterfeit Parts *Fraudulent/Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition*



- Electronic parts should be purchased, whenever possible, directly from OCMs or from authorized suppliers
- Independent distributors should be used only after consideration of alternate parts, redesign, schedule adjustments and a reasonable search for material from authorized (franchised) sources has been conducted and approval has been obtained from a designated author
- OCMs and distributors (authorized (franchised) and independent) should be required to provide certificates of conformance and acquisition supply chain traceability; otherwise the purchaser assumes unknown risks
 - Note: such documentation has the potential to be forged or falsified
- Acquisition supply chain traceability consists of the name and location of all supply chain intermediaries from the part manufacturer to the direct source of the product
- The organization should ensure that these requirements are clearly stated as deliverable data within the procurement documents, regardless of which level of the supply chain provides the parts
- If supply chain traceability is unknown or documentation is suspect, appropriate risk mitigation should be used as described in this document.



Implementation Challenges

- Parts availability - lead time
- Obsolete parts
- Impact on Socio-Economic supplier goals
- Flow-down and implementation by sub-tier suppliers
- Commercial Off-the-Shelf (COTS) Products
- Impact on Program Cost

Summary

- There are many risks in the supply chain
- With the globalization of the supplier base, increased attention needs to be placed on processes that control procurement
- Standards such as AS9100 make it clear that organizations are responsible for the conformity of the product, irrespective of where or how it is obtained.

AS9100C paragraph 7.4.1