SAE 2014 Aerospace Systems and Technology Conference

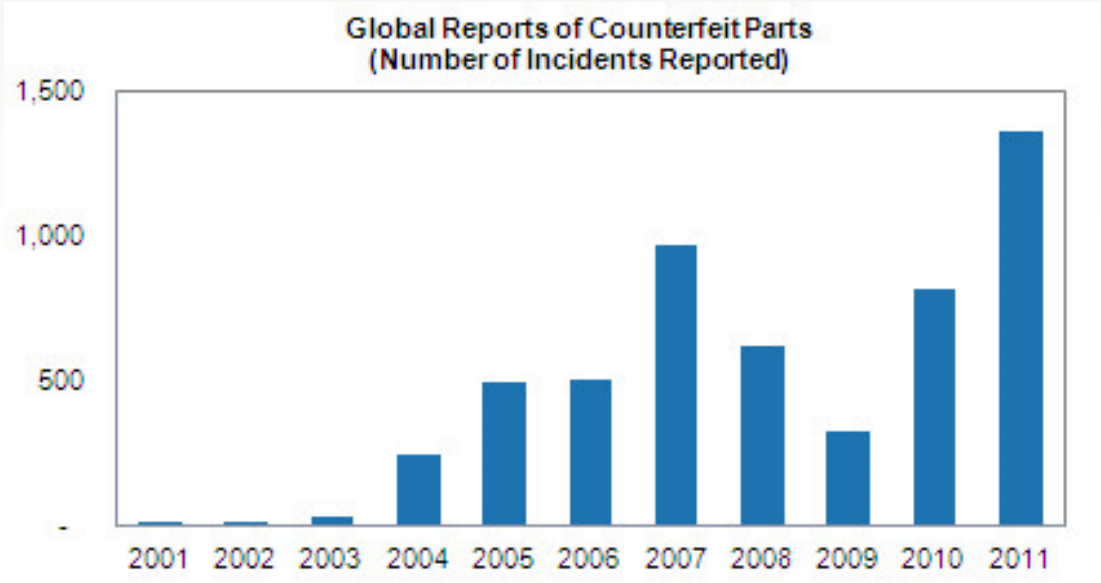
September 24, 2014

Answering the Demands of NDAA Section 818 and the DFARS Rule on Detection & Avoidance of Counterfeit Electronic Parts

Robert S. Metzger
Rogers Joseph O'Donnell, P.C.
750 Ninth Street, N.W., Ste 710
Washington, D.C. 20001
(202) 777-8951
rmetzger@rjo.com www.rjo.com

A BRIEF HISTORY

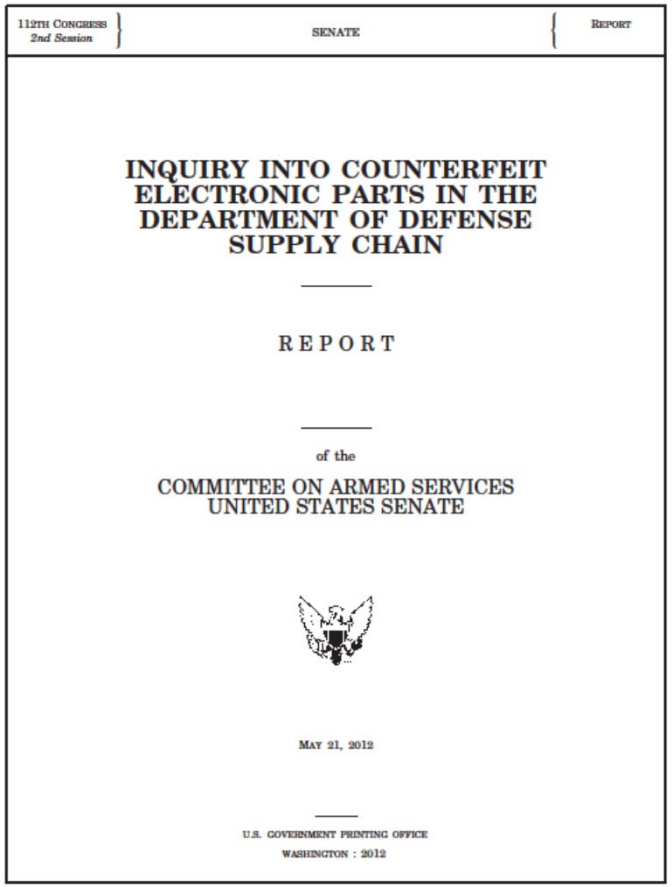
Counterfeits: A Growing Threat



Source: IHS Parts Management
Figures represent ERAI Suspect Counterfeit or High Risk Part Incidents and GIDEP Suspect Counterfeit Alerts for electronic components

Senate Armed Services Committee hearings in 2011 focused attention on the threat and prompted Congress to "legislate supply chain security" through Section 818 of NDAA 2012

SASC Investigation & Findings



112TH CONGRESS 2nd Session | SENATE | REPORT

INQUIRY INTO COUNTERFEIT ELECTRONIC PARTS IN THE DEPARTMENT OF DEFENSE SUPPLY CHAIN

REPORT

of the

COMMITTEE ON ARMED SERVICES
UNITED STATES SENATE

MAY 21, 2012

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON : 2012

Key SASC findings:

- **China is the dominant source country for counterfeit electronic parts;**
- **The Chinese government has failed to take steps to stop counterfeiting operations;**
- **DoD lacks knowledge of the scope and impact of counterfeit parts on critical defense systems;**
- **The use of counterfeit parts in defense systems can compromise performance, reliability and safety of military personnel;**
- **Industry's reliance on unvetted independent distributors results in unacceptable risks;**
- **Weaknesses in the testing regime for electronic parts creates vulnerabilities; and**
- **The defense industry routinely failed to report cases of suspect counterfeit parts.**

The Result: Section 818 FY 2012 NDAA

Section 818 Operates At Many "Junctions" of the Supply Chain

- Detection
- Exclusion
- Enforcement
- **Purchasing Practices**
- **Inspection & Testing**
- **Reporting**
- Corrective Measures
- **Contractor Systems**
- Costs & Incentives
- Sanctions

Section 818 Addresses Only Counterfeit *Electronic Parts.*
The Statute Applies Only to DoD Primes and High-Tier Subs
– but not the DFARS regulations

Fundamental Requirements of Section 818

818(c) (3) TRUSTED SUPPLIERS.—The revised regulations issued pursuant to paragraph (1) shall—

(A) require that, **whenever possible**, the Department and Department contractors **and subcontractors at all tiers**—

(i) obtain electronic parts that are in production or currently available in stock **from the original manufacturers** of the parts or their authorized dealers, or from trusted suppliers who obtain such parts exclusively from the original manufacturers of the parts or their authorized dealers; and

(ii) obtain electronic parts that are not in production or currently available in stock from **trusted suppliers**;

(B) establish requirements for **notification** of the Department, and **inspection**, **testing**, and **authentication** of electronic parts that the Department or a Department contractor or subcontractor obtains from **any source other** than a source described in subparagraph (A);

(C) establish **qualification requirements**, consistent with the requirements of section 2319 of title 10, United States Code, pursuant to which the Department may **identify trusted suppliers** that have appropriate policies and procedures in place to detect and avoid counterfeit electronic parts and suspect counterfeit electronic parts; and

(D) authorize Department contractors and subcontractors to identify and use **additional trusted suppliers**, provided that—

(i) the standards and processes for identifying such trusted suppliers comply with established **industry standards**;

(ii) the contractor or subcontractor assumes responsibility for the authenticity of parts provided by such suppliers as provided in paragraph (2); and

(iii) the **selection** of such trusted suppliers is **subject to review and audit** by appropriate Department officials.

(e) IMPROVEMENT OF CONTRACTOR SYSTEMS FOR DETECTION AND AVOIDANCE OF COUNTERFEIT ELECTRONIC PARTS.—

(1) IN GENERAL.—Not later than 270 days after the date of the enactment of this Act, the Secretary of Defense shall implement a program to enhance contractor detection and avoidance of counterfeit electronic parts.

(2) ELEMENTS.—The program implemented pursuant to paragraph (1) shall—

(A) require covered contractors that supply electronic parts or systems that contain electronic parts to **establish policies and procedures** to eliminate counterfeit electronic parts from the defense supply chain, which policies and procedures shall address—

(i) the **training** of personnel;

(ii) the **inspection** and **testing** of electronic parts;

(iii) processes to abolish counterfeit parts **proliferation**;

(iv) mechanisms to enable **traceability** of parts;

(v) use of **trusted suppliers**;

(vi) the **reporting** and **quarantining** of counterfeit electronic parts and suspect counterfeit electronic parts;

(vii) **methodologies** to **identify** suspect counterfeit parts and to rapidly determine if a suspect counterfeit part is, in fact, counterfeit;

(viii) the design, operation, and maintenance of **systems to detect and avoid** counterfeit electronic parts and suspect counterfeit electronic parts; and

(ix) the **flow down** of counterfeit avoidance and detection requirements to subcontractors; and

(B) establish processes for the **review and approval of contractor systems** for the detection and avoidance of counterfeit electronic parts and suspect counterfeit electronic parts, which processes shall be comparable to the processes established for contractor business systems under section 893 of the Ike Skelton National Defense Authorization Act for Fiscal Year 2011.

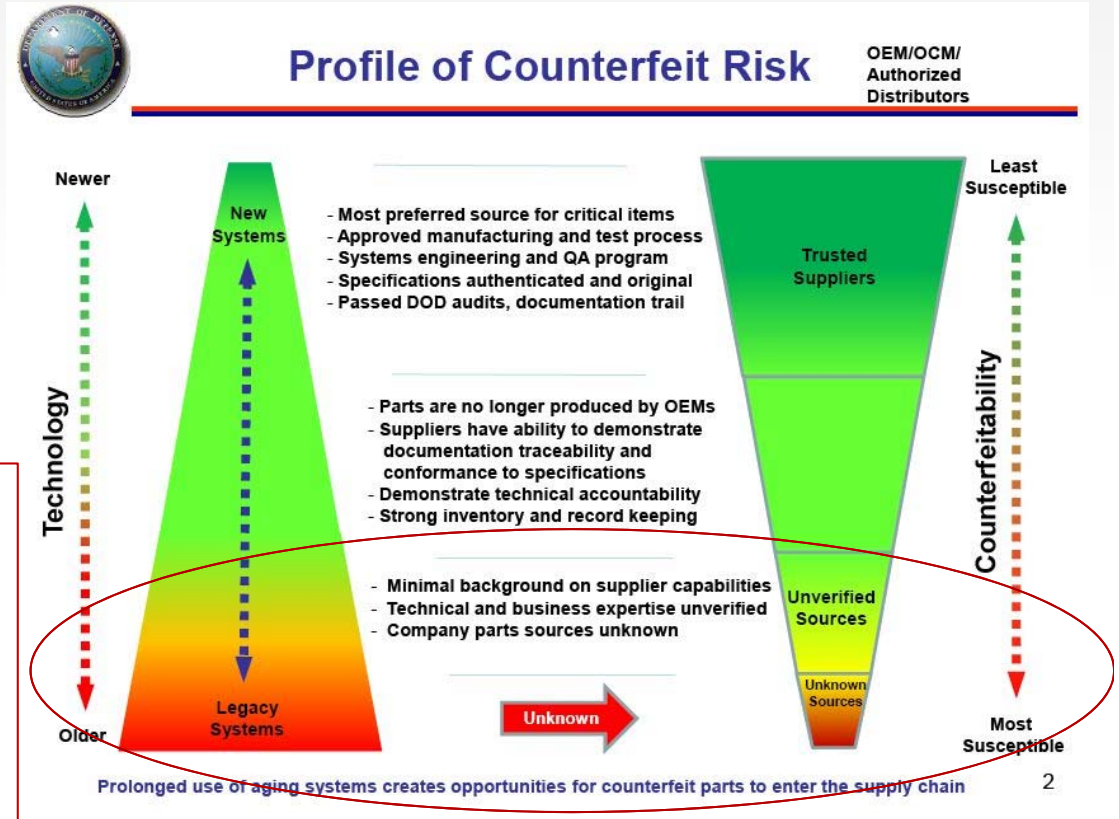
Section 818's Primary Target: *Fakes*

The principal motivation for counterfeit parts, addressed by Section 818, is profit.

Bad actors seek to answer demand for scarce parts by offering well-priced fakes that appear genuine -- but are not.

Demand is greatest for parts that are obsolete, out of production and no longer available from OCMs or authorized distributors.

DoD is vulnerable because of the long life of legacy systems that still require support



"Taints" Are The Greater Threat – But Less Likely

"Counterfeit electronic part"

" … 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."

"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.**"

DFARS 202.101 DEFINITION

Counterfeit: *Substandard or non-functional; risk to operations & reliability; methods exist to detect (in most cases)*

Electronic part*: implies cyber physical security issues and concerns of tainted hardware.*

"Taint"

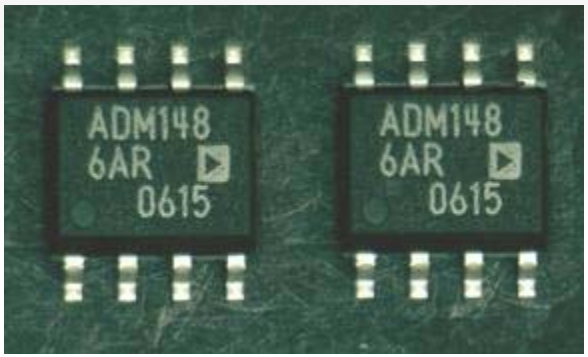
"sabotage, maliciously introduce unwanted functions, or otherwise subvert … a system in order to conduct surveillance or to deny access to, disrupt, or otherwise degrade its reliability or trustworthiness."

Common Criteria Supply Chain Technical Working Group, DRAFT "Supply Chain Security Assurance" April 2012, available at http://www.commoncriteriaportal.org/

Unexpected Functionality
Potentially Latent Functions
Vector to induce or exploit cyber attack
Risk of unauthorized extraction
Threat to critical systems and mil ops

Can be very difficult to detect

The Threat of Cloned Parts is Real



"Recent DoD and U.S. interest in counterfeit parts has resulted in the identification of widespread introduction of counterfeit parts into DoD systems through commercial supply chains. Since many systems use the same processors and those processors are typically built overseas in untrustworthy environments, **the challenge to supply chain management in a cyber- contested environment is significant**."

DEFENSE SCIENCE BOARD:
Resilient Military Systems and the Advanced Cyber Threat
(January 2013, at p.4)

- Examples have been identified of cloned, recent vintage electronic parts
  - From major suppliers
  - Of significant complexity
  - That mimic electrical functionality
- Clones are produced by illegal but highly capable enterprises
- Detection of clones is both costly and difficult – but not impossible

The existence of clones points to greater risk that hostile actors will insert harmful code using clones as carriers

Responses to “Fakes” & “Taints” - Overview

- Interim (but effective) regulations of November 2013 implement Sec. 806 of FY 2011 NDAA and allow DoD to act on threat information to exclude high-risk suppliers.
- Insertion of a “malicious” counterfeit part could be used to vector a cyber attack through the supply chain.
- The new DFARS will have some prophylactic benefit to avoid or deter “taints” though (a) narrowing the supply chain and (b) enhanced test and inspection.
- Special challenge is presented to avoid “taints” from critical applications and trusted systems and networks.

THE NEW DFARS
79 Fed. Reg. 26092 (May 6, 2014)

DFARS Structure

- Part 202 – Definitions
- Part 231 – Contract Cost Principles and Procedures
- Part 244 – Subcontracting Policies and Procedures
- Part 246 – Quality Assurance
  - Subpart 246.8 – Contractor Liability for Loss of or Damage to Property of the Government [CPSR]
  - DFARS 246.870 Contractors' counterfeit electronic part detection and avoidance systems [12 criteria]
- Part 252 – Solicitation Provisions and Contract Clauses
  - DFARS 252.244–7001 Contractor Purchasing System Administration
  - DFARS 252.246–7007 Contractor Counterfeit Electronic Part Detection and Avoidance System

Key Features of the DFARS

1) Contractors subject to the rule ("**covered contractors**") must **establish and maintain systems** to detect and avoid counterfeit electronic parts. The adequacy of these systems will be measured against **twelve criteria**.

2) An emphasis is placed upon practices that will **improve the traceability** of electronic parts so that customers are able to know a part's history and chain of custody.

3) DoD will oversee and administer the contractor systems as part of "**Contractor Purchasing System Reviews**," part of the larger program to monitor "business systems" of larger suppliers.

4) Contractors are strongly encouraged to **use original sources (OEMs and OCMs), whenever possible**, but are provided no guidance on how they should qualify other sources if needed parts are not available from the sources considered most trusted.

5) **Notification** and **additional test and inspection** is required for parts not from the most trusted sources, using "risk-based" methods, though factors and criteria for these methods are not well articulated.

6) Companies must take care to identify both **suspect and confirmed** counterfeit electronic parts and to give **notification** when discovered.

7) Costs of replacing counterfeits are **unallowable** for larger companies that do cost-based contracting with DoD, as are the costs of rework and corrective action.

8) Suspect and confirmed counterfeit electronic parts must be **quarantined and reported** to appropriate authorities and measures must be taken to avoid their being returned into the supply chain.

9) Companies are to improve **training**, make greater use of industry **standards** and keep **informed** on reported counterfeit incidents and on new counterfeiting information and trends.

10) DoD contractors subject to the regulation are required to **flow down** counterfeit detection and avoidance requirements to **all levels** in the supply chain.

System Criteria

DFARS 252.246–7007 Contractor Counterfeit Electronic Part Detection and Avoidance System

(1) Training

The training of personnel.	**Contractors have flexibility.** **Training should be tailored for function/ responsibility.** **Refresh needed to recognize new STDs, etc.** **Should a covered contractor confirm subs conduct training also?**

(2) Inspection and Testing

The inspection and testing of electronic parts, including criteria for acceptance and rejection. Tests and inspections shall be performed in accordance with accepted Government- and industry-recognized techniques. Selection of tests and inspections shall be based on minimizing risk to the Government. Determination of risk shall be based on the assessed probability of receiving a counterfeit electronic part; the probability that the inspection or test selected will detect a counterfeit electronic part; and the potential negative consequences of a counterfeit electronic part being installed (e.g., human safety, mission success) where such consequences are made known to the Contractor.	Publication of AS-6171 will be important as it provides a hierarchy of test methods and provides a mechanism for risk-based analysis with needed detail. AS-6171 examines Risk as to the Supplier (R_S), as to the Component (R_C) and as to the Product (R_P) and takes into account Adjustment factors that recognize how each risk area may be mitigated. This is an objective method for contractors to make risk-informed decisions as to what additional measures of test and inspection are appropriate and cost-effective where electronic parts cannot be obtained from preferred, authorized sources such as OCMs and authorized distributors. However, contractors still will face situations where they do not and cannot know the intended or eventual utilization of a given part. Nor are contractors assured of having relevant knowledge of "threat" relevant to risk of receiving a counterfeit.

(3) Proliferation

Processes to abolish counterfeit parts proliferation.	**Responsible contractors know they must avoid the "return" of a counterfeit electronic part into the supply chain.** **Difficulties arise where a contractor deals with brokers/distributors or test labs who have ownership and possession of parts found suspect or counterfeit. Does the "covered contractor" have control over the disposition?** **Also, it may be difficult to establish which party is responsible for reporting the counterfeit.**

(4) Traceability

Processes for maintaining electronic part traceability (e.g., item unique identification) that enable tracking of the supply chain back to the original manufacturer, whether the electronic parts are supplied as discrete electronic parts or are contained in assemblies. This traceability process shall include certification and traceability documentation developed by manufacturers in accordance with Government and industry standards; clear identification of the name and location of supply chain intermediaries from the manufacturer to the direct source of the product for the seller; and where available, the manufacturer's batch identification for the electronic part(s), such as date codes, lot codes, or serial numbers. If IUID marking is selected as a traceability mechanism, its usage shall comply with the item marking requirements of 252.211-7003, Item Unique Identification and Valuation.	Traceability is obviously desirable but this criteria likely will be very difficult to meet for many parts that covered contractors have in inventory and acquire. Today, only a limited class of MIL SPEC (PRF) parts come with end-to-end traceability and these represent only a modest (if not small) fraction of the universe of parts that an aerospace and defense contractor will employ. While traceability will improve as new demands become regular practices, it will not be possible to satisfy the literal words ("back to the original manufacturer") for many parts and it would not be cost-effective or practicable only to use parts that have full traceability. A contractor should be found compliant if it seek all available documentation of pedigree or provenance and considers the extent of documentation when it is necessary to perform a risk-based assessment of a particular source for an electronic part. Certainly, the absence of traceability is a factor (R_C) that may indicate additional inspection and test.

(5) Use of Suppliers

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.	**A core (and inarguable) principle of the DFARS is that the best way to avoid counterfeits is to procure parts from OCMs, other authorized manufacturers or authorized distributors. However, DoD must support many legacy systems where required parts are obsolete or no longer available from these trusted sources.** **The DFARS is short on guidance on how to qualify additional sources when necessary. Contractors may be informed by Standards and best practices to make prudent, risk informed decisions.**

(6) Reporting & Quarantining

Reporting and quarantining of counterfeit electronic parts and suspect counterfeit electronic parts. Reporting is required to the Contracting Officer and to the Government-Industry Data Exchange Program (GIDEP) when the Contractor becomes aware of, or has reason to suspect that, any electronic part or end item, component, part, or assembly containing electronic parts purchased by the DoD, or purchased by a Contractor for delivery to, or on behalf of, the DoD, contains counterfeit electronic parts or suspect counterfeit electronic parts. Counterfeit electronic parts and suspect counterfeit electronic parts shall not be returned to the seller or otherwise returned to the supply chain until such time that the parts are determined to be authentic.	The principle that counterfeit and suspect electronic parts should be quarantined is important for several reasons, most important to prevent re-entry, but also to enable appropriate investigation and law enforcement activity. Reporting is a more complex subject. Presently, a rule is pending ("Expanded Reporting of Nonconforming Items") that would broadly impose new reporting obligations for non-conforming (and counterfeit) electronic parts and other material. The outcome of this new rule will figure into a compliant reporting mechanism for the purposes of the DFARS. There are a number of complications as concerns reporting. Not all actors in the supply chain have access to GIDEP. Questions also will arise as to which party is responsible to make the report where several tiers of companies are involved in a particular transaction

(7) Identification

Methodologies to identify suspect counterfeit parts and to rapidly determine if a suspect counterfeit part is, in fact, counterfeit.	**SAE Standards will figure prominently, along with other industry standards, in selection among compliant methodologies for this purpose.** **One challenge is present in that the definition of "electronic part" in the DFARS "includes any embedded software or firmware." There is no present Standard or commonly available and accepted method to make this determination for most parts.** **Costs are another consideration.**

(8) Systems to Detect & Avoid

Design, operation, and maintenance of systems to detect and avoid counterfeit electronic parts and suspect counterfeit electronic parts. The Contractor may elect to use current Government- or industry-recognized standards to meet this requirement.	**Covered contractors and companies that accept flowdown must develop compliant systems and will be subject to review against the 12 criteria.** **The DFARS recognizes the importance of but does not specify particular industry Standards.** **There will be many challenges. A key issue is whether the DCMA will administer assessment of contractor systems flexibly to accommodate the enormous diversity of contractor circumstances. At the same time, contractors want to know the standards for oversight and want assurance of consistency.** **Also "TBD" is whether higher tier companies must audit or otherwise verify their subs.**

(9) Flowdown

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.	**While a commendable objective, flowdown is beset with serious implementation challenges. Legally, Section 818 and the DFARS apply only to "covered contractors" – about 1,200 companies subject to all of DoD's Cost Accounting Standards. The flowdown requirement, however, attempts to force those "covered contractors" to obtain the same anti-counterfeit assurance (and system compliance) from all sources in its supply chain – including COTS and commercial item sources and small business. There are 23,000 companies that sell to DoD.** **Practically, we will see that significant supply sources refuse full flowdown, accept only limited flowdown or offer their own measures as surrogates. DoD's interests will not be served if it interprets and applies the flowdown requirement to mean that its "covered contractors" cannot use their low-risk, established sources should they decline less than full flowdown.**

(10) Keeping Informed

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.	**This is not a particularly difficult requirement, conceptually, though companies at lower tiers of the supply chain may have some difficulty keeping informed and other companies, for whom aerospace and defense market are not significant, may have insufficient motivation.** **A general problem is that counterfeiters continue to "evolve" by using new and more sophisticated techniques. The Government may be the best source of this information – as well as the potentially classified information about threats of "maliciously encoded" or tampered parts – but mechanisms to share such sensitive information are limited.**

(11) Screening GIDEP & Other Reports

Process for screening GIDEP reports and other credible sources of counterfeiting information to avoid the purchase or use of counterfeit electronic parts.	**Conceptually, this is not an objectionable requirement, but as applied through flowdown to lower tier companies, and to commercial sources and COTS suppliers, it likely will be problematic.** **TBD is how to identify and rapidly exploit various government and private databases (e.g., ERAI), and how to resolve potential inconsistencies in reported info.** **Ultimately, data analytics should be used to rapidly process information to "adjudicate" source risks. How will the many sources of data be aggregated, vetted and made accessible?**

(12) Control of Obsolete Parts

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.	**There are many DoD programs (e.g., PPP, DMSMS) and company initiatives to deal with obsolescence, as matters of design, sustainment, engineering and purchasing practices.** **However, the value of this 12th criteria is only prospective and it does nothing to help industry deal with the present and very real problem of how to satisfy continuing requirements for parts that already are obsolete or out of production.** **A related issue is how to treat inventory that was accumulated before these new rules came in force.**

CRITICAL IMPLEMENTATION ISSUES

Highest Risk Areas

Subject / Source of Requirement	Compliance Risk	Business Risk
Contract Flow Down **246-870-2(b)(9)** **252.246-7007(c)(9)** **252.246-7007(e)**	DFARS requires flow down to subcontractors at all levels and there is no exception for COTS or commercial suppliers or small business. But "covered contractors" do not have the legal right to impose the DFARS upon non-covered suppliers who refuse or insist on modification. Potentially an issue for CPSR if 100% flowdown not achieved.	Some necessary suppliers may refuse any flowdown and others will insist on limited flowdown or negotiations. Covered contractors will need to establish procedures to address flowdown issues and perform risk-based assessment of whether to proceed with sources that object. Flowdown may impose liability risks on companies greater than contract value. Potential uncertainty as to how to deal with exceptions.
Use of suppliers other than the original mfg. **246-870-2(b)(5)** **252.246-7007(c)(5)**	DFARS expresses a strong preference for EEE parts from "trusted sources" but defers guidance on how to qualify parts from other ("additional") suppliers who are needed as not all current requirements can be met from original sources. Contractors need to establish risk-based methods to qualify sources; unknown is whether and when the Government must be informed and whether approval is required. Note that Sec. 824 NDAA 2015 may resolve.	Production stoppage or impaired sustainment could result if the sourcing mandate prohibiting the use of brokers or parts from other than OCMs and Authorized Distributors. Potentially significant additional costs to develop and implement internal procedures for qualification of additional sources. Covered contractors may seek to shift business risk to testing distributors. EEE supply may be more expensive due to constricted base.
Legacy Inventory / DFARS Applicability (Preamble)	DFARS Comment indicates that inventory not procured in connection with a previous DoD contract is subject to traceability and authentication requirements. Rule itself is silent on inventory, but issue is present what practices are expected of a compliant system, in order to pass CPSR.	Legacy inventory bought from brokers or kept in common stores must be re-evaluated in accordance with current standards. Additional risk assessment and test and inspection will be required. Continuity of supply and sustainment at risk if contractors cannot employ inventory after reasonable measures to assess and address risk.
Traceability **252.246-7007(c)(11)**	Supply chain unable to support traceability requirement as written "clear identification of the name and location of supply chain intermediaries from the manufacturer to the direct source of the product for the seller". No guidance on what to do (e.g. waiver) where traceability is absent. Risk of disapproval of CPP system.	"End to end" traceability is contrary to contemporary practices and documentation cannot be created if not existent. It may be costly to obtain such documentation in the future and some sources (e.g., COTS, commercial) may decline. EEE parts sourced from brokers or distributors will remain needed but will not have the documentation sought; existing inventory presents a similar problem. Practical solution necessary.

Intermediate Risk Areas

Subject / Source of Requirement	Compliance Risk	Business Risk
COTS & COMMERCIAL SOURCES **Applicability (Preamble)**	DFARS applies to COTS and commercial sources and small businesses – some of which will not accept but remain necessary EEE sources. Uncertain extent to which disclosure is required or consent. Covered contractor may be held responsible to verify DFARS compliance by all downstream sources. DCMA approach for CPSR not now certain.	Some necessary suppliers may reject conditions or requirements or increase costs to justify. Business risk may include interruption or loss of necessary sources of supply. Potential costs for redesign or contract manufacture. May be reduced competition. BUT – risk of counterfeits from many COTS and commercial suppliers is low – risk may be acceptable. Fewer small businesses may be qualified sources.
DCMA CPSR Surveillance **252.246-7007(d)** **246.870-2** **252.244-7001**	CPSR is used to assess and validate whether system criteria are satisfied. Standards and process to be used by DCMA are unknown. Whether DCMC will accommodate contractor-specific solutions t/b/d. It is not now known how DCMA will treat known implementation issues, e.g., flowdown, traceability, qualification of additional suppliers. Unknown if DCMA would consider an escape a deficiency. Consistency of DCMA oversight is uncertain.	All existing contracts with DFARS 252.242-7005 Contractor Business Systems invoked. It is unknown what DCMA would consider a deficiency significant enough to invoke penalties – but DCMA has a review process. Will be additional nonrecurring and recurring allowable costs to develop and implement improved systems. Recovery of those costs is uncertain. An unsatisfactory system could result in a failed Purchasing System and reduce payments.
Allowable Costs for Counterfeit & Suspect Counterfeit **231.205-71**	CAS-Covered contractors could be exposed to penalties for expressly unallowable costs if the Govt is charged for costs of a counterfeit or suspect cost or for rework or corrective action. Additional risk present for costs reported from vendors and subcontractors.	CAS-covered contractors will need means to identify and segregate potentially unallowable costs and to restore costs if a part is found not counterfeit . Can be difficult to establish standards and process to distinguish among parts "known counterfeit," "suspect," "other nonconforming" or where classification cannot be made.
Reporting & Quarantining **246-870-2(b)(6)&(b)(11)** **252.246-7007(c)(6)&(c)(11)**	It will be difficult to segregate items destined for DoD due to dual-use and common items. Covered contractor could be at risk if vendor does not report or quarantine. Note that DOD IG "requires" disclosure of any counterfeit even if contractor's system worked as intended to identify and prevent.	There will be commercial issues as to quarantining especially if a covered contractor does not accept delivery of a suspect or counterfeit part from a third party source. Legal issues may be present as to payment and accuracy of reporting. **Proposed FAR would expand reporting of nonconforming items to "common items" and applies to all government agencies.**

CONCLUSION

Importance of SAE Standards

- Section 818 and the DFARS obligate defense suppliers to implement new systems to detect and avoid counterfeit parts
- But neither the statute nor the regulations inform industry as to "how" this is to be done.
- Evidence thus far is that DoD does not intend to issue "prescriptive" requirements or mandate practices.
- Instead, it is likely DoD will look to responsible companies to develop their own systems.
- Adherence to SAE and other relevant standards will be seen as providing assurance of system compliance.
- The pending AS6171 will prove especially important because it introduces new taxonomy for risk analysis.

Speaker: Robert S. Metzger

Robert S. Metzger received his B.A. from Middlebury College and is a graduate of Georgetown University Law Center, where he was an Editor of the *Georgetown Law Journal*. He was a Research Fellow, Center for Science & International Affairs, Harvard Kennedy School of Government.

Mr. Metzger is the head of the Washington, D.C. office of Rogers Joseph O'Donnell, P.C. He is a member of the International Institute for Strategic Studies (IISS), London. Academic publications on security topics include articles in *International Security*, the *Journal of Strategic Studies* and *Indian Defence Review*. He is a Vice-Chair of the Supply Chain Assurance Committee of TechAmerica. He is recognized as a leading expert on supply chain assurance and cyber risk management. He is ranked in 2014 *Chambers USA* as a top Government Contracts lawyer (national).

Rogers Joseph O'Donnell is a boutique law firm that has specialized in public contract matters for 33 years. It is ranked in "Band 2" by the 2014 *Chambers USA* – the only boutique among the nine highest ranked firms. Mr. Metzger advises leading US and international companies on key public contract compliance challenges and in strategic business pursuits.

SELECTED EXTERNAL PUBLICATIONS

available at http://www.rjo.com/metzger.html

- "Making the Best of the Final DFARS re Counterfeit Parts," ERAI *Insights* Newsletter, Q2 2014
- "Convergence of Counterfeit and Cyber Threats: Understanding New Rules on Supply Chain Risk," *Federal Contracts Report*, Feb. 18, 2014
- "DoD Counterfeit Parts Rule – So Little After So Long," *Law360* , Jun. 5, 2013
- "Counterfeit Electronic Parts: What to Do Before The Regulations (and Regulators) Come? (Part 2)," *Federal Contracts Report*, Aug. 21, 2012
- "Counterfeit Electronic Parts: What to Do Before the Regulations (And Regulators) Come? (Part 1)," *Federal Contracts Report*, Jun. 21, 2012 (with Jeff Chiow)
- "Legislating Supply Chain Assurance: Examination of Section 818 of the FY 2012 NDAA," *The Procurement Lawyer*, Vol. 47, No. 4 (with Jeff Chiow)