Supply Chain Security:
DFARS – Detection & Avoidance of Counterfeit Electronic Parts
March 22, 2017

Robert S. Metzger
Rogers Joseph O'Donnell, P.C.
875 Fifteenth Street, N.W., Ste 725
Washington, D.C. 20005
(202) 777-8951
www.rjo.com

Coverage

- Fundamentals:
  - The *threat* of counterfeit electronics
  - The *statute* - Section 818 NDAA FY 2012
  - The *DFARS* – Detection & Avoidance of Counterfeit Electronic Parts – **Revised August 2016**
    - *What* the Rule requires … *Who* is subject to the Rule … *How* it is implemented
- Advanced Topics:
- Policies and Procedures for Compliance
  - The 12 "System Criteria"
  - Key Implementation Challenges

This presentation reflects Mr. Metzger's personal views and should not be attributed to any client of his firm or organization with which he is involved or affiliated.

POLLING SLIDE - 1

Who are you currently employed by?

A) Government agency

B) Contractor - Large business

C) Contractor - Small business

D) Contractor - Socio-economic set-aside category (e.g., 8(a), Service-Disabled Veteran Owned)

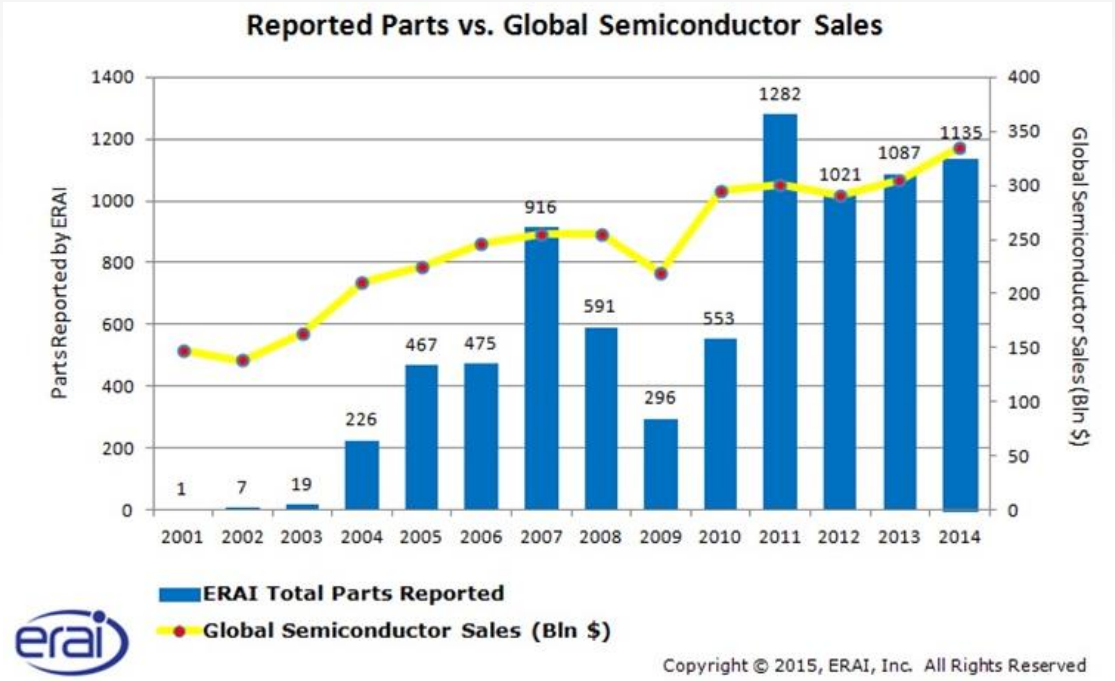
E) Non-profit

F) Law Firm

G) Other (I'm looking!)

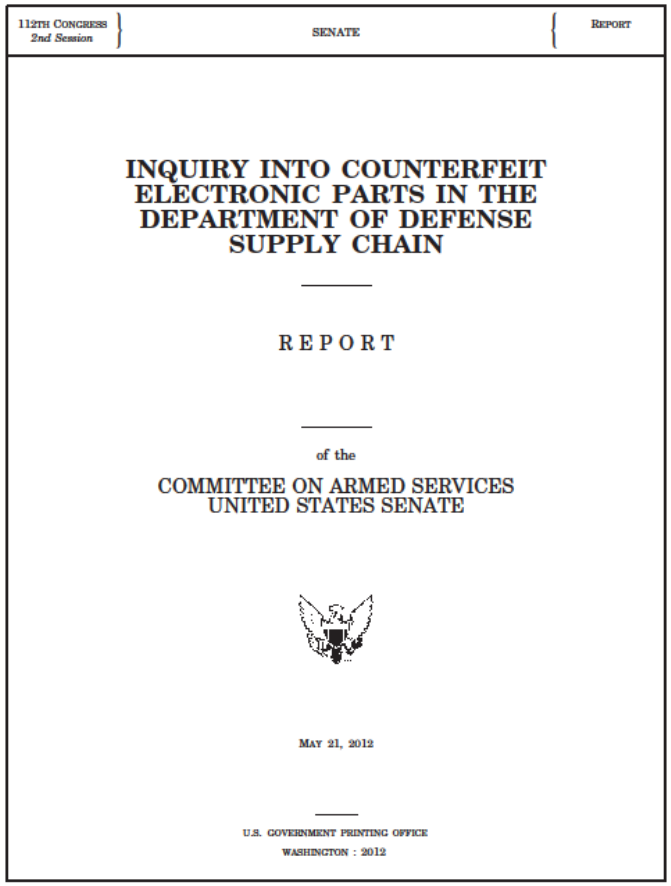
Why
Laws and Rules to Detect & Avoid Counterfeit Electronic Parts

SASC Investigation of Counterfeit Parts



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

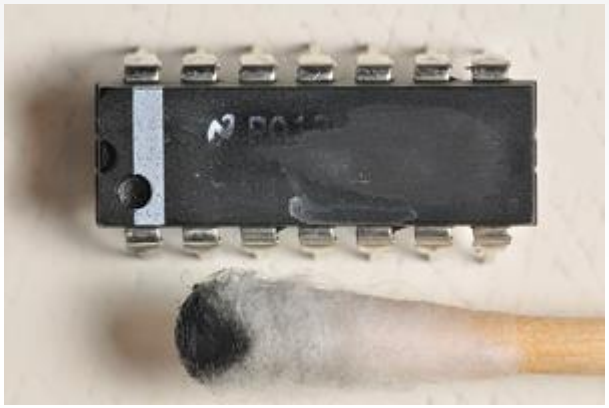
MAY 21, 2012

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.

Section 818's Primary Target: *Fakes*

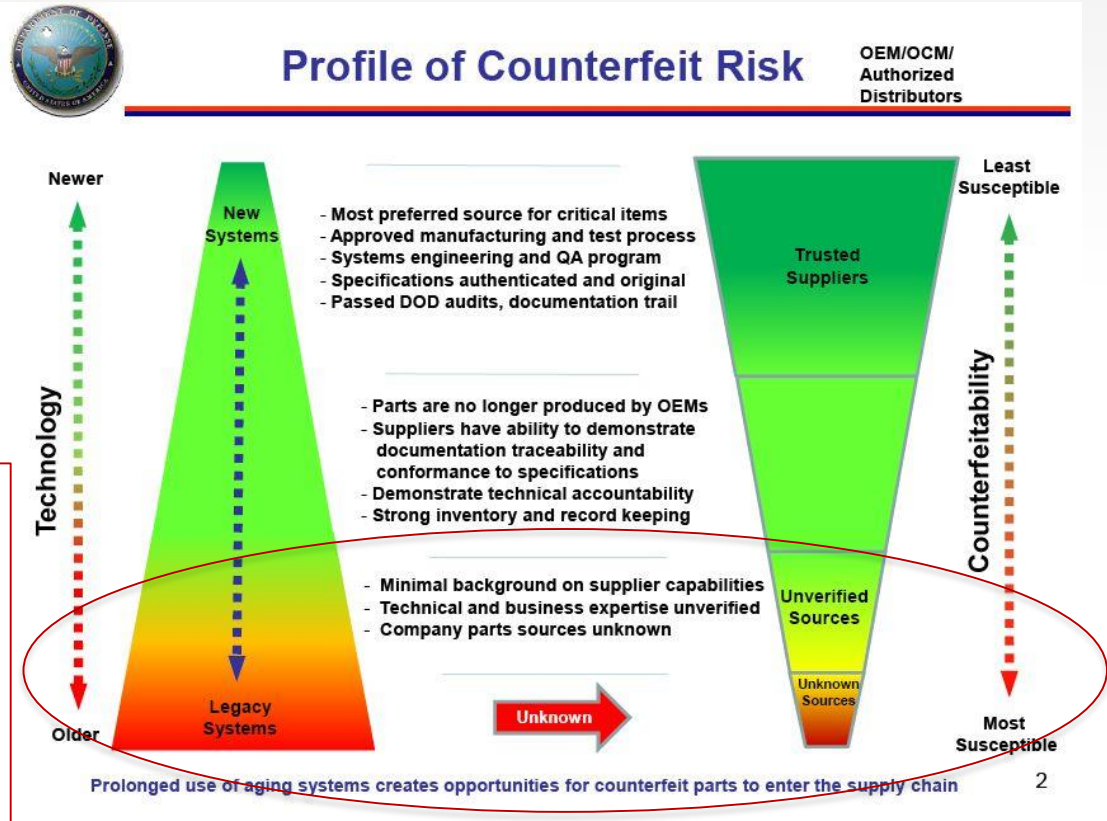


The principal motivation for counterfeit parts, addressed by Section 818, is profit.

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.

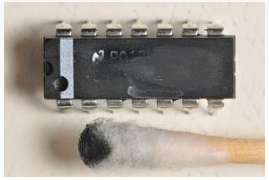
DoD is vulnerable because of the long life of legacy systems that still require support



DoD depends upon deployed systems where sustainment requires access to out-of-production electronic parts

"Fakes" vs. "Taints" (Cyber/physical)

The Ordinary ("Fake") Counterfeit Part:



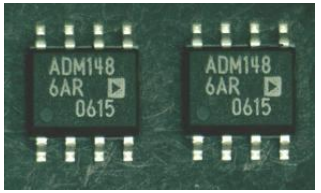
Substandard or non-functional
Likely to fail in intended environment
Presents risk to operations & reliability
Methods exist to detect (in most cases)
Injury :

- **degradation of performance**
- **diminished reliability**
- **potential device/system failure**
- **burden on support & sustainment**
- **costs of "remediation"**

Typically a counterfeit electronic part contains no active mechanism that can be exploited by an adversary.

Focus of 818 and DFARS is on "Fakes"

"Taint"



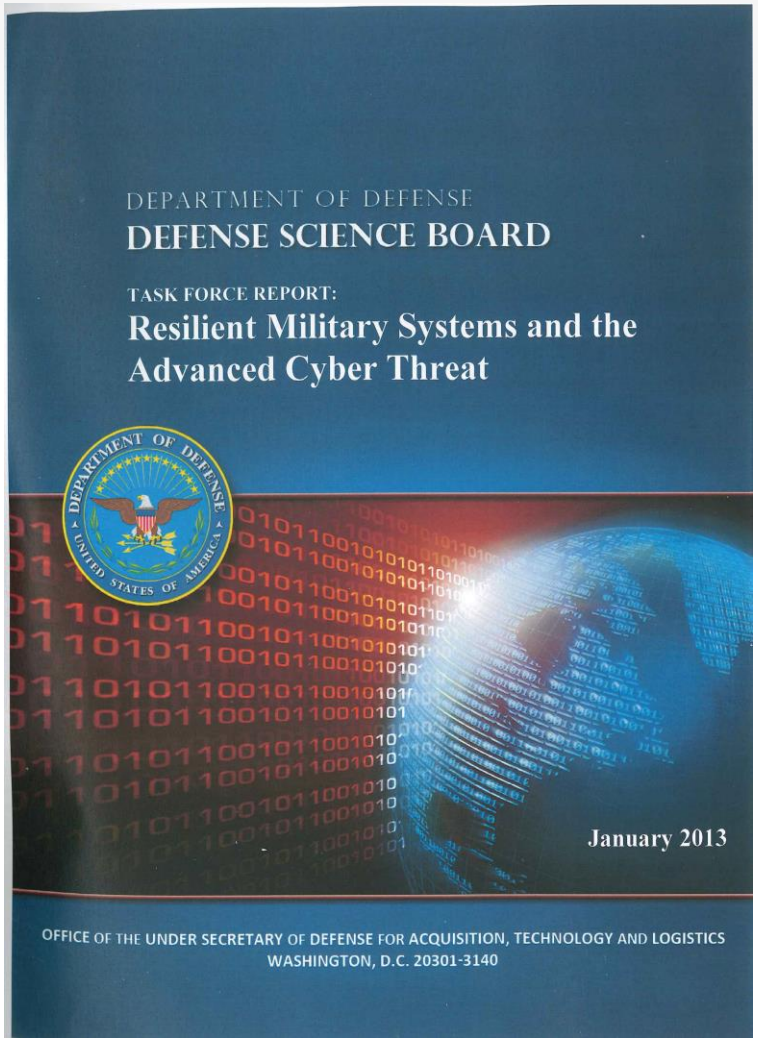
"sabotage, maliciously introduce unwanted functions, or otherwise subvert … a system in order to conduct surveillance or to deny access to, disrupt, or otherwise degrade its reliability or trustworthiness."

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

"Exploitation of vulnerabilities in microelectronics and embedded software can cause mission failure in modern weapons systems. Such exploitations are especially pernicious because they can be difficult to distinguish from electrical or mechanical failures and because effects can run the gamut from system degradation to system failure to system subversion."

Defense Science Board, *Cyber Supply Chain*, Feb. 2017

Cyber Risk is present in Supply Chain Vulnerability



"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."

"DoD is in the process of institutionalizing a Supply Chain Risk Management (SCRM) strategy that prioritizes scarce security resources on critical mission systems and components, provides intelligence analysis to acquisition programs and incorporates vulnerability risk mitigation requirements into system designs."

(at p.4)

DSB Cyber Supply Chain Report (Feb. 2017)

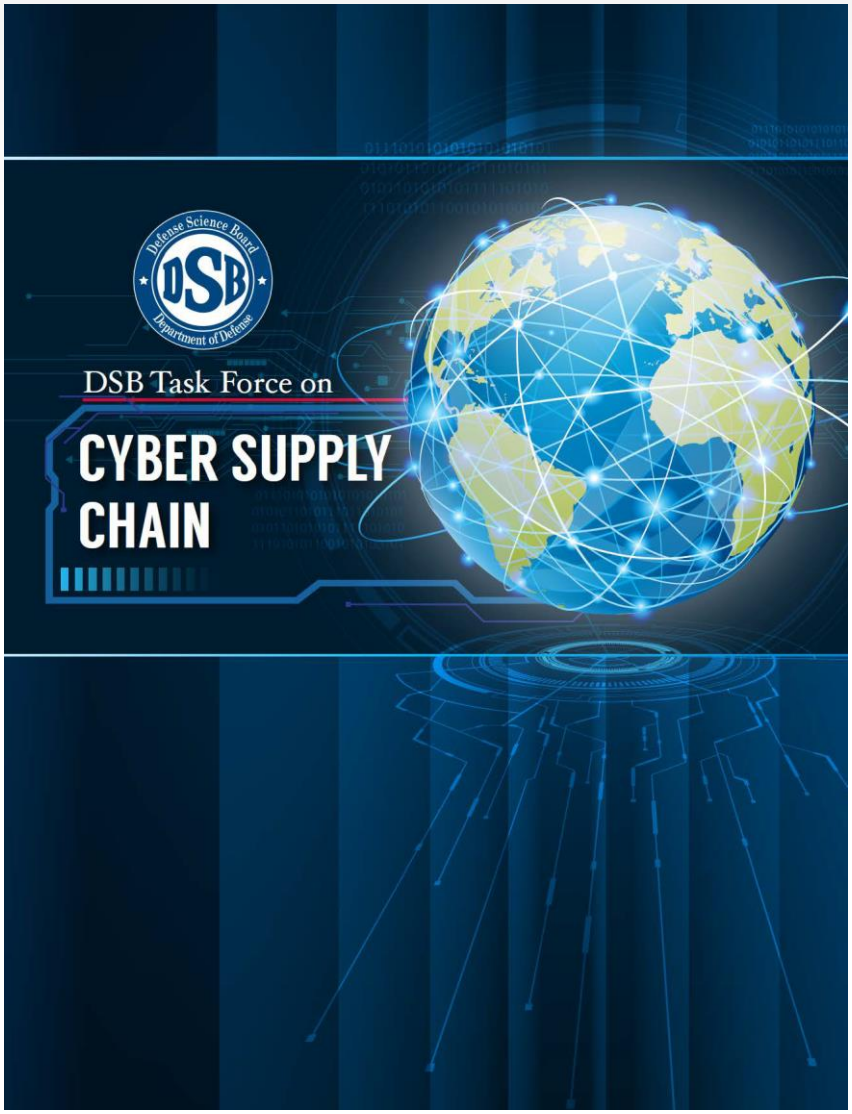
"The task force observed instances that may have been unsuccessful attacks on critical weapons systems via malicious insertion. It is difficult to know whether such activity is widespread, but **the existence of counterfeit electronics in the supply chain demonstrates the potential for such at**tacks. When done effectively, malicious insertion will not be detectible until actuated and it may present as a design flaw when ultimately observed." p.2

"Reporting of counterfeit and "suspect-counterfeit" microelectronics is mandatory for some, but not all prime contracts and subcontracts. **Such reporting requirements are inconsistent and no DoD system at present collects event information on cyber-physical attacks of electronic components** as its primary function. To address these concerns, a shared vulnerability database and a parts application database of installed hardware could promulgate corrective actions across weapons systems." p.4

"The continued discovery of counterfeit parts in the DoD supply system is proof that criminal activity (with less sophistication than a nation-state adversary) can succeed in penetrating supply chains. **Parts provenance in sustainment is harder to track than in acquisition**, and there are opportunities for an attacker to gain access." p.7

"While the DFARS has utility to respond to the "physical" threat that a counterfeit part may not perform as an authentic part would, this **DFARS does not now address the distinct software of firmware threat** to cyber-active parts." p.15

"There **is no consistent or assured means to authenticate provenance or pedigree of parts currently in production** by reference to embedded authentication or traceability information." p.41



POLLING SLIDE - 2

Why are you taking this course?

A) For CPE credit
B) For general knowledge of counterfeit parts
C) For detailed knowledge of counterfeit parts
D) My job is to implement these regs and practices
E) Expecting a Government compliance review
F) Need a diversion from other responsibilities

NDAA FY 2012
SECTION 818

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 CAS-covered DoD contractors.
The DFARS regulations require flow down to "all subcontractor tiers"

Features of Section 818

Applies to "covered contractors who supply electronic parts or products that include electronic parts" 818(c)(2)(A)

Costs of rework or corrective action "required to remedy the **use or inclusion** of counterfeit electronic parts are **not allowable**" 818(c)(2)(B) – not limited to costs on supply

"whenever possible, [DoD] contractors and subcontractors at all tiers" are to obtain electronic parts from trusted suppliers 818(c)(3)(A)

reporting requirement applies to "any Department contractor or subcontractor who becomes aware …" of a counterfeit 818(c)(4)

§ 818: Trusted Suppliers, Contractor Systems

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.

Evolution of § 818: Trusted Suppliers

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~~ suppliers identified as trusted suppliers in accordance with regulations issued pursuant to subparagraphs (C) and (D) 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 suppliers identified as trusted suppliers in accordance with the regulations issued pursuant to subparagraphs (C) and (D); and~~trusted suppliers~~;

~~ii.~~ iii. obtain electronic parts from alternate suppliers when such parts are not available from original manufacturers, their authorized dealers, or trusted suppliers;

(B) establish requirements for notification of the Department, and for 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 ~~clause (i) or (ii) of~~ subparagraph (A), when obtaining the electronic parts in accordance with such clauses is not possible~~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 as trusted suppliers those that have appropriate policies ~~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 their own identified trusted suppliers'~~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.

◀NDAA 2015 § 817

Experience has shown that insistence upon "trusted suppliers" is not workable in an environment where sustainment demands access to other but less trustworthy sources.

NDAA 2017 § 806

"The House amendment contained a provision (sec. 806) that would modify section 818 of the National Defense Authorization Act for Fiscal Year 2012 (Public Law 112-81) by replacing the term "trusted suppliers" with the term "suppliers that meet anticounterfeiting requirements", as well as related conforming amendments. This provision would clear up confusion about the term, which refers to the specific category of microelectronics supplies that have been accredited by the Defense Microelectronics Activity."

(Conference Report)

Section 818: Contractor Systems

(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 – Amendments

- Focus on “covered contractors” (those subject to CAS)*
- Costs of counterfeit, rework or corrective action unallowable
- Regulations required all tiers of DoD suppliers to use “trusted suppliers”*
- Required covered contractors to establish policies and procedures to address nine areas, including traceability*, use of trusted suppliers*, flowdown*

NDAA 2013 § 833

* Changed by new 2016 regs

- Costs allowable if DoD-approved system, parts = GFP + prompt report

NDAA 2015 § 817

- Modified “trusted suppliers” and allowed buying from “alternate suppliers”

NDAA 2016 § 885

- Eased criteria for allowable costs; added DoD approval of “additional suppliers”

NDAA 2017 § 806

- Replaces “trusted suppliers” with “suppliers that meet anticounterfeiting requirements”

DFARS
Detection & Avoidance of Counterfeit Electronic Parts

August 2016 DFARS Changes

In August 2016, DoD made important changes to the DFARS rules on detection and avoidance of counterfeit electronic parts. The revised rules introduce new flexibility in the use of sources other than the OEM (or authorized distributor) and reduce the liability risks to contractors if a counterfeit escape occurs. Even more emphasis is given to industry standards and the regs elaborate upon traceability. Yet, key parts of the revised regulations need clarification. Further, **the DFARS continue to rely upon a "transactional" focus** rather than a systems approach that could produce superior SCRM results.

Bloomberg BNA — Federal Contracts Report™

Counterfeit Parts

Even if everyone in the supply chain accepts this proposition as correct, the Defense Department's sustainment challenge requires the servicing of thousands of items of aging equipment where the electronic parts necessary for maintenance *are not* available from any "trusted supplier."

Changes to Counterfeit Parts Regulations Merit Review, Revision to Industry Practices

By Robert S. Metzger

Late in 2011, Congress enacted Section 818 to the National Defense Authorization Act (NDAA) of fiscal 2012. Final Defense Federal Acquisition Regulation Supplement (DFARS) Rules, "Detection and Avoidance of Counterfeit Electronic Parts," were issued May 6, 2014. The objective of Section 818 was to improve both Defense Department (DOD) and industry practices in the detection and avoidance of counterfeit electronic parts. Section 818 was a remarkable statute in several respects. It sought to influence the practices of the defense supply chain at multiple junctures, including detection, exclusion, enforcement, purchasing practices, inspection and testing, reporting, corrective measures, contractor systems and sanctions.

Ordinarily, when Congress tries by legislation to change the intricacies of how DOD does business with its suppliers, frustration is likely to overcome accomplishment. Here, however, the fundamental "logic" of Section 818 has held up well over the 2½ years of experience that government and industry have accumulated since enactment. The DFARS has resulted in efforts, especially by the larger defense contractors, to create, document and maintain systems to detect and avoid counterfeit electronic parts. Industry has recognized, broadly, that electronic parts should be procured from original sources, where available, and much has been accomplished in the development of new standards and best practices to assist both purchasers and suppliers.

Robert S. Metzger, rmetzger@rjo.com, heads the Washington, D.C., office of Rogers Joseph O'Donnell, PC, a boutique law firm specializing in public contracts. A frequent contributor to Federal Contracts Report, Bob was named a 2016 "Federal 100" awardee by Federal Computer Week for his contributions to cyber and supply chain security. This article reflects Mr. Metzger's personal views and should not be attributed to any client of his firm or organization with which he is involved or affiliated.

My article on the DFARS revisions appears in *Federal Contracts Report*, 106 FCR 423, 10/25/16, *available at* http://www.rjo.com/PDF/FCR_10252016RSM.pdf.

The DFARS Structure: Then / Now

Final Rule: "Detection and Avoidance of Counterfeit Electronic Parts"

- **Subpart 202 – Definitions* definitions added and revised**
- **Subpart 212 – COTS – now requires -7008 "Sources of Electronic Parts" clause**
- **Subpart 231 – Contract Cost Principles and Procedures* revised**
- **Subpart 242 – Contract Admin. – adds review of "contractor-approved suppliers"**
- **Subpart 244 – Subcontracting Policies and Procedures (CPSR)** (rvw "CPDAS")
- **Subpart 246.8 – Government Property**
  - Subpart 246.8 – Contractor Liability for Loss of or Damage to Property of the Government * significant changes – inc'g 3 risk-related "Tiers" of supplier preference
  - DFARS 246.870 Contractors' counterfeit electronic part detection and avoidance systems [12 criteria] * *traceability and "use of suppliers"* criteria changed
- **Subpart 252 – Solicitation Provisions and Contract Clauses**
  - DFARS 252.244–7001 Contractor Purchasing System Administration * unchanged
  - DFARS 252.246–7007 Contractor Counterfeit Electronic Part Detection and Avoidance System *
  - DFARS 252.246-7008 Sources of Electronic Parts * new, required, inc'g commercial items

Considerations for Service Providers

Subcontracting Policies & Procedures

ACO is responsible for reviews of contractor's ***purchasing system****; review is to include "*the adequacy the contractor's counterfeit electronic part detection and avoidance system under DFAR 252.246-7007"

A service provider subject to purchasing system review would be likely to receive scrutiny of the adequacy of its CPDAS

Contract Cost Principles

"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 are unallowable." [except if a "safe-harbor" is available]* DFARS 231.205-71(b)

Applies to all companies subject to the DFAR Cost Principles – not limited to companies that supply parts, assemblies or systems

Contract Clause

Per 246.870-3(a)(1)(iii), the -7007 clause (CPDAS) is to be used in solicitations and contracts when procuring … "**[s]ervices where the contractor will supply electronic parts or components, part, or assemblies containing electronic parts as part of the service**."

(The clause does not apply to small bus set-asides.)

A service provider subject to CAS could be found obligated to flow down to subcontractors at all levels of the supply chain" the CPDAS contract clause.

Part 202: Key Definitions

"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."*

"Suspect counterfeit electronic part"

*"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."*

"Obsolete electronic part"

*"an electronic part that is **no longer ~~in production by~~** available from the original manufacturer or an authorized aftermarket manufacturer* [defined separately]*"*

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."~~*

"Contractor-approved supplier"

"means a supplier that does not have a contractual agreement with the original component manufacturer for a transaction, but has been identified as trustworthy by a contractor or subcontractor"

(NEW)

DFARS 202.301 Contract Clauses for Commercial Items

(C) Use the clause at 252.246-7008, Sources of Electronic Parts, as prescribed in 246.870-3(b), to comply with section 818(c)(3) of Pub. L. 112-81, as amended by section 817 of the National Defense Authorization Act for Fiscal Year 2015 (Pub. L. 113-291).

SUBPART 246.8—CONTRACTOR LIABILITY FOR LOSS OF OR DAMAGE TO PROPERTY OF THE GOVERNMENT

246.870-3 Contract clauses

(b) Use the clause at 252.246-7008, Sources of Electronic Parts, in solicitations and contracts, including solicitations and contracts using FAR part 12 procedures for the acquisition of commercial items, when procuring—
(1) Electronic parts;
(2) End items, components, parts, or assemblies containing electronic parts; or
(3) Services, if the contractor will supply electronic parts or components, parts, or assemblies containing electronic parts as part of the service.

DFARS 231.205-71 (Cost Principle)

(b) The costs of counterfeit electronic parts and suspect counterfeit electronic parts … are unallowable, unless—

(1) The contractor has an operational system to detect and avoid counterfeit electronic parts and suspect counterfeit electronic parts that has been reviewed and approved by DoD pursuant to 244.303;

(2) The counterfeit electronic parts or suspect counterfeit electronic parts are Government-furnished property as defined in FAR 45.101 or were obtained by the contractor in accordance with the clause at 252.246-7008, Sources of Electronic Parts; and

(3) The contractor—

(i) Becomes aware … through inspection, testing, and authentication efforts of the contractor or its subcontractors; through a Government Industry Data Exchange Program (GIDEP) alert; or by other means; and

(ii) Provides timely (i.e., within 60 days after the contractor becomes aware) written notice to ~~the Government~~—

(A) The cognizant contracting officer(s); and

(B) GIDEP (… unless the electronic part is the subject of an on-going criminal investigation).

DFARS 246: Contractors Counterfeit Electronic Parts Detection and Avoidance System

Additional definition…

"**Authorized supplier**," as used in this subpart, means a supplier, distributor, or an aftermarket manufacturer with a contractual arrangement with, or the express written authority of, the original manufacturer or current design activity to buy, stock, repackage, sell, or distribute the part.

The three "Tiers" of source preference

"Tier 1" – lowest risk supplier

DFARS 246.870-2 **Policy**.

(a) *Sources of electronic parts.*

(1) Except as provided in paragraph (a)(2) of this section, the Government requires contractors and subcontractors at all tiers, to—

(i) Obtain electronic parts that are in production by the original manufacturer or an authorized aftermarket manufacturer or currently available in stock from—

(A) The original manufacturers of the parts;

(B) Their authorized suppliers; or

(C) Suppliers that obtain such parts exclusively from the original manufacturers of the parts or their authorized suppliers; and

DFARS 246: Contractors Counterfeit Electronic Parts Detection and Avoidance System

"Tier 2" – medium-risk supplier

(ii) Obtain electronic parts that are not in production by the original manufacturer or an authorized aftermarket manufacturer, and that are not currently available in stock from a source listed in paragraph (a)(1)(i) of this section, from suppliers identified by the Contractor as contractor-approved suppliers, provided that—

(A) For identifying and approving such contractor-approved suppliers, the contractor uses established counterfeit prevention industry standards and processes (including inspection, testing, and authentication), such as the DoD-adopted standards at https://assist.dla.mil;

(B) The contractor assumes responsibility for the authenticity of parts provided by such contractor-approved suppliers (see 231.205-71); and

(C) The selection of such contractor-approved suppliers is subject to review and audit by the contracting officer.

DFARS 246: Contractors Counterfeit Electronic Parts Detection and Avoidance System

"Tier 3" – highest-risk supplier

(2) The Government requires contractors and subcontractors to comply with the notification, inspection, testing, and authentication requirements of paragraph (b)(3)(ii) through (b)(3)(iv) of the clause at 252.246-7008, Sources of Electronic Parts, if the contractor—

(i) Obtains an electronic part from—

(A) A source other than any of the sources identified in paragraph (a)(1) of this section, due to nonavailability from such sources; or

(B) A subcontractor (other than the original manufacturer) that refuses to accept flowdown of this clause; or

(ii) Cannot confirm that an electronic part is new or not previously used and that it has not been comingled in supplier new production or stock with used, refurbished, reclaimed, or returned parts.

DFARS 246: Other Changes

Government-furnished parts

(3) Contractors and subcontractors are still required to comply with the requirements of paragraphs (a)(1) or (2) of this section, as applicable, if—

(i) Authorized to purchase electronic parts from the Federal Supply Schedule;

(ii) Purchasing electronic parts from suppliers accredited by DMEA; or

(iii) Requisitioning electronic parts from Government inventory/stock under the authority of the clause at 252.251-7000.

(A) The cost of any required inspection, testing, and authentication of such parts may be charged as a direct cost.

(B) The Government is responsible for the authenticity of the requisitioned electronic parts. If any such part is subsequently found to be counterfeit or suspect counterfeit, the Government will—

(*1*) Promptly replace such part at no charge; and

(*2*) Consider an adjustment in the contract schedule to the extent that replacement of the counterfeit or suspect counterfeit electronic parts caused a delay in performance.

Mandatory Use of the New -7008 Clause - *252.870-3(b)*

(b) Use the clause at 252.246-7008, Sources of Electronic Parts, in solicitations and contracts, including solicitations and contracts using FAR part 12 procedures for the acquisition of commercial items, when procuring—

(1) Electronic parts;

(2) End items, components, parts, or assemblies containing electronic parts; or

(3) Services, if the contractor will supply electronic parts or components, parts, or assemblies containing electronic parts as part of the service.

For CAS-covered contractors [-7007 Clause}

Items (4) and (5) of the 12 System Criteria are changed

(4) Risk-based processes ~~for maintaining electronic part traceability (e.g., item unique identification)~~ that enable tracking of ~~the supply chain~~ electronic parts ~~back to~~ from the original manufacturer to product acceptance by the Government, whether the electronic parts are supplied as discrete electronic parts or are contained in assemblies, in accordance with paragraph (c) of the clause at 252.246-7008, Sources of Electronic Parts (also see paragraph (c)(2) of this clause). ~~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.~~

(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~~ in accordance with the clause at 252.246-7008

Systems Clause (-7007) does not apply to small business set asides

DFARS 252.246-7008 Sources of Electronic Parts NEW

For use when procuring all electronic parts, including commercial items (252.870-3(b))

(b) *Selecting suppliers*. In accordance with section 818(c)(3) of the National Defense Authorization Act for Fiscal Year 2012 (Pub. L. 112-81), as amended by section 817 of the National Defense Authorization Act for Fiscal Year 2015 (Pub. L. 113-291), the Contractor shall—

(1) **First** obtain electronic parts that are in production by the original manufacturer or an authorized aftermarket manufacturer or currently available in stock from—

(i) The original manufacturers of the parts;

(ii) Their authorized suppliers; or

(iii) Suppliers that obtain such parts exclusively from the original manufacturers of the parts or their authorized suppliers;

(2) **If electronic parts are not available as provided in paragraph (b)(1)** of this clause, obtain electronic parts that are not in production by the original manufacturer or an authorized aftermarket manufacturer, and that are not currently available in stock from a source listed in paragraph (b)(1) of this clause, from suppliers identified by the Contractor as **contractor-approved suppliers**, provided that—

(i) For identifying and approving such contractor-approved suppliers, the Contractor uses established counterfeit prevention industry standards and processes (**including inspection, testing, and authentication**), such as the DoD-adopted standards at https://assist.dla.mil;

(ii) The Contractor **assumes responsibility** for the authenticity of parts provided by such contractor-approved suppliers; and

(iii) The Contractor's selection of such contractor-approved suppliers is **subject to review and audit** by the contracting officer; **or**

(3)(i) Take the actions in paragraphs **(b)(3)(ii) through (b)(3)(iv)** of this clause if the Contractor—

(A) Obtains an electronic part from—

(1**) A source other than any of the sources identified in paragraph (b)(1) or (b)(2)** of this clause, due to nonavailability from such sources; or

(2) A **subcontractor** (other than the original manufacturer) **that refuses to accept flowdown** of this clause; or

(B**) Cannot confirm** that an electronic part **is new or previously unused** and that it **has not been comingled** in supplier new production or stock with used, refurbished, reclaimed, or returned parts.

(ii) If the contractor obtains an electronic **part** or cannot confirm an electronic part pursuant to paragraph (b)(3)(i) of this clause—

(A) Promptly **notify** the Contracting Officer in writing. If such notification is required for an electronic part to be used in a designated lot of assemblies to be acquired under a single contract, the Contractor may submit one notification for the lot, providing identification of the assemblies containing the parts (e.g., serial numbers);

(B) Be **responsible for inspection, testing, and authentication**, in accordance with existing applicable industry standards; and

(C) Make **documentation** of inspection, testing, and authentication of such electronic parts **available** to the Government upon request.

DFARS 252.246-7008 … Traceability (NEW)

For use when procuring all electronic parts, including commercial items (252.870-3(b))

(c) Traceability. If the Contractor is not the original manufacturer of, or authorized supplier for, an electronic part, the Contractor shall—

(1) Have risk-based processes (taking into consideration the consequences of failure of an electronic part) that enable tracking of electronic parts from the original manufacturer to product acceptance by the Government, whether the electronic part is supplied as a discrete electronic part or is contained in an assembly;

(2) If the Contractor cannot establish this traceability from the original manufacturer for a specific electronic part, be responsible for inspection, testing, and authentication, in accordance with existing applicable industry standards; and

(3)(i) Maintain documentation of traceability (paragraph (c)(1) of this clause) or the inspection, testing, and authentication required when traceability cannot be established (paragraph (c)(2) of this clause) in accordance with FAR subpart 4.7; and

(ii) Make such documentation available to the Government upon request.

DFARS 252.246-7008 … Flowdown

For use when procuring all electronic parts, including commercial items (252.870-3(b))

(e) *Subcontracts*. The Contractor shall include the substance of this clause, including this paragraph (e), in subcontracts, including subcontracts for commercial items that are for electronic parts or assemblies containing electronic parts, unless the subcontractor is the original manufacturer.

POLLING SLIDE - 3

Do you have Systems to Detect & Avoid Counterfeit Electronic Parts?

A) No – we are thinking about it

B) No – we are working on it

C) Yes – we are looking to validate or improve

D) Not sure we need one

E) Hope we are not required to

Policies & Procedures
to Detect & Avoid Counterfeit Electronic Parts

Policies and Procedures for Compliance

Overview

As we've discussed:

- Counterfeit parts avoidance and detection is an area of **business and legal risk**
- Prudent aerospace and defense contractors should establish **rule-based compliance programs** for counterfeit parts avoidance and detection.
- Measures must be **cost-effective** and **enable** not defeat business opportunity and contract performance

Goal: mitigate risk to the business and align with DoD's expectations. This is easier said than done. (We have helped companies do this.)

Policies and Procedures for Compliance

Tenets of Effective Counterfeit Part Avoidance & Detection Practices

- **Supplier Selection.** Practices should prioritize purchase of electronic components from OEMs or their authorized distributors. **In addition**, efforts "contractor-approved suppliers" should be established and utilized.
- **Risk-based actions.** Purchases from "Tier 2 or 3" cannot be avoided entirely, but special practices are needed for inspection, test and authentication.
- **Notify.** When suspect counterfeits are encountered, practices should obligate notification to relevant stakeholders, both Government and industry.

Policies and Procedures for Compliance

Section 818(e) lists the key components of a robust counterfeit parts compliance program. *See* Slide 17. In drafting policies and procedures for compliance, due regard must be given to each of the following:

(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 / suspect counterfeit electronic parts

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

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

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

Each of the 12 System Criteria will be discussed subsequently.

Policies and Procedures for Compliance

Resources for Contractors

- **Section 818; the DFARS; DCMA–INST 1205** (July 2015)
- **Key industry standards such as:**
  - **SAE Aerospace Standard AS5553** ("Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition")
  - **SAE Aerospace Standard AS6081** ("Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition – Distributors")
  - **SAE Aerospace Standard AS6171** ("Test Methods Standard; General Requirements, Suspect/Counterfeit, Electrical, Electronic, and Electromechanical Parts") (in ballot)
  - **IDEA 1010 Standard** (Independent Distributors of Electronics Association) ("Acceptability of Electronic Components Distributed in the Open market")
- **GIDEP** (Government-Industry Data Exchange Program) (www.gidep.org)
- **ERAI** (www.erai.com)
- **Other Government Resources:**
  - **Mil-Std-1580** for DPA (Destructive Physical Analysis)
  - **Mil-Std-883** Visual Inspection Criteria for testing microelectronic devices

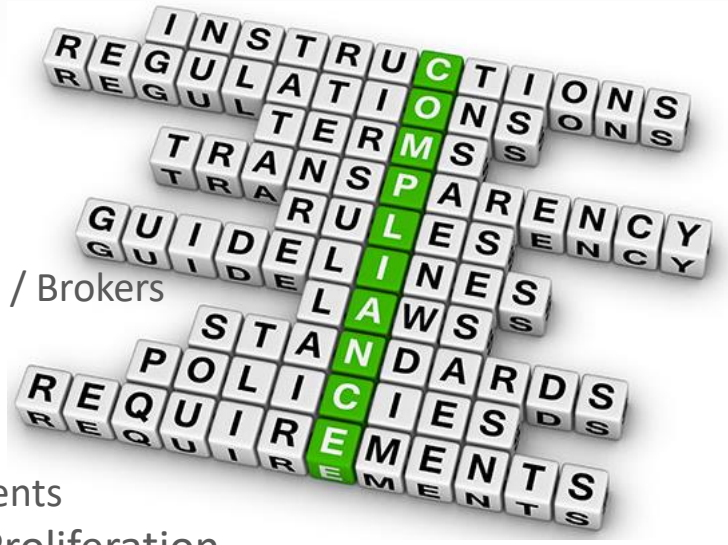
DLA QTSL-5961/5962 Dec. 2012
Criteria and Provisions for Qualified Testing Suppliers List (QTSL)

DLA QSLD-5961/5962 Mar. 2014
Criteria and Provisions for Qualified Suppliers List of Distributors (QSLD)

Policies and Procedures for Compliance

Sample Compliance Policy Outline

I. Purpose & Scope
II. Reference Material
III. Definitions
IV. Procedures
  A. Overview & Objectives
  B. Trusted Sources
  C. Trustworthy Suppliers, Independent Distributors / Brokers
  D. Expectations of Suppliers
  E. Purchasing Practices
  F. Control of Obsolete Parts
  G. Inspection / Acceptability of Electronic Components
V. Suspect or Confirmed Counterfeit; Avoiding Proliferation
VI. Warranty
VII. Purchase Order Terms and Conditions & Subcontract Flow-downs
VIII. Reporting & Notification
IX. Costs
X. Training & Audits



Compliance Issues to Consider

- Flowdown & Supply Chain Assurance
- COTS & Commercial Suppliers
- Protection by Contract (T&C)
- Treatment of Inventory
- Prime Contractor Obligations
- “Leveraged” Supplier Apprv’l
- Value Chain Diligence
- “Pedigree”, “Provenance” & Traceability
- Obsolescence & DMSMS

- “Trustworthy Sources”
- Standards & Best Practices
- Testing & Technical Measures (Selection, Basis, Resources)
- Who, When & What to Report
- Responding to “CEP” Events
- Compliance Documentation
- DCMA Oversight (Risk Level)
- Potentially Unallowable Costs
- Cooperation w/ Enforcement

POLLING SLIDE - 4

If you have a system to Detect & Avoid Counterfeit Electronic Parts

A) Have you been reviewed and approved by DoD?

B) Have you been reviewed and approved by a Prime?

C) Have you identified and reported any counterfeit or suspect counterfeit electronic parts?

D) Have you had to repair, replace or rework any equipment because of counterfeit electronic parts?

E) None of these apply to me

Twelve System Criteria
DFARS 252.246–7007(c)(1-12)

(1) Training

The training of personnel.	**Contractors have flexibility. Training should be tailored for function/ responsibility. Refresh is needed because of the many changes in the Aug. 2016 DFARS and as new standards (AS 6171, etc.) come on line.** **Training should be tailored for the functional area. E.g., Purchasing (Supply Chain), QA, Contracts, Compliance, 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.

It is the purchaser's responsibility under AS-6171 to supply the information that drives the risk assessment; it is the purchaser's responsibility to decide upon the test and assurance measures.

Today, there are no DoD-mandated criteria to inform contractors on how to select tests and inspection and how to address the costs of higher level and potentially destructive tests.

The new SAE AS-6171 provides a hierarchy of test methods and provides a mechanism for risk-based analysis with needed detail. It 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 and potential mitigation measures for each risk area. This is an objective method for contractors to make risk-informed decisions. Because necessary electronic parts *cannot always* be obtained from preferred, authorized sources such as OCMs, standards to guide industry and government are critical.

In fact, the new -7008 clause requires use of "established counterfeit prevention industry standards and processes (including inspection, testing, and authentication" for "Tier 2" contractor-approved suppliers and for "Tier 3" parts the acquiring contractor is both "responsible for inspection, testing, and authentication, in accordance with existing applicable industry standards" and must make documentation of these available to the Government.

(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? Is the "covered contractor" legally responsible?**
It is essential to secure, by contract, authority over the disposition of parts determined to be suspect or counterfeit; under no circumstances should risk be accepted that such parts may be returned to the supply chain.	**The "anti-proliferation" requirement in the -7007 ("systems") clause applies to CAS-covered contractors. There is no counterpart in the -7008 ("sources") clause that flows down to all (but COTS) suppliers.**
	However, -7007(e) calls upon "covered contractors" to "include the substance of this clause" (flow down) in subcontracts. It is recommended that subcontracts establish positive obligations of suppliers to prevent proliferation.

(4) Traceability

Risk-based processes that enable tracking of electronic parts from the original manufacturer to product acceptance by the Government, whether the electronic parts are supplied as discrete electronic parts or are contained in assemblies, in accordance with paragraph (c) of the clause at 252.246-7008, Sources of Electronic Parts (also see paragraph (c)(2) of this clause).	**While desirable, achieving traceability to satisfy this criteria will be very difficult for many parts now in inventory. 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.** **The new JESD243 microelectronics standard for counterfeit electronic parts includes little of the information needed for end-to-end traceability.** **"Risk-based processes" may be problematic if the contractor has no knowledge of the component use in unit, system, platform, etc. Assembly-level traceability is different functionally from parts.** **Traceability will improve as new demands become regular practices and as new standards and best practices emerge. But it is not be possible to demonstrate traceability "back to the original manufacturer" for many parts.** **-7008(c) requires "tracking" (physical provenance?) from OEM to product acceptance (feasible how often and for whom?) and more "inspection, testing and authentication when traceability cannot be established".**

(5) Use of Suppliers

Use of suppliers in accordance with the clause at 252.246-7008.

(Previously – in May 2014 DFARS:

"Use of suppliers that are the original manufacturer, 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."

Sophisticated contractors likely will "neck down" sources of supply and emphasize ("leverage") entities that they qualify as "contractor-approved suppliers". These may include non-stocking distributors.

This criteria has undergone material change both to § 818 and in the DFARS.

Originally, the emphasis was on "trusted suppliers" – a term now-abandoned. It remains true, however, that the best way to avoid counterfeits is to procure parts from OCMs, other authorized manufacturers or authorized distributors. However, DoD's contractors *must* support many *legacy systems* where required parts are obsolete or no longer available from these trusted sources.

The DFARS in Pt. 246 and in the -7008 ("sources") clause now "admit" to additional "contractor-approved suppliers" and "permit" use of other parts but the regulations are clear more in concept than in practical detail. Contractors should be informed by standards and best practices to make prudent, risk informed decisions – should document their decisions – and may seek CO guidance/approval.

(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 to prevent re-entry and to enable appropriate investigation and law enforcement activity. In practice, however, many in industry are reluctant to report and seek to avoid responsibility. Moreover, the existing process is slow and poorly informs potentially at-risk operators of equipment.** **Reporting is a more complex subject. Today, there is *no clear guidance* on who is to report "suspect" or "counterfeit" electronic parts (and no guidance whatsoever specific to "taints"). The DFARS apply only to "covered contractors" but counterfeits may be discovered by others in the supply chain, e.g., distributors or test labs, and they are *not* subject to the DFARS. Companies continue to perceive that reporting even a "find" of a counterfeit to GIDEP or ERAI has a "negative" connotation (rather than demonstrating a strong system). GIDEP is not a strong vehicle (today). The new DSB Cyber Supply Chain Study recommends funding for GIDEP improvements.**

(7) Identification

Methodologies to identify suspect counterfeit parts and to rapidly determine if a suspect counterfeit part is, in fact, counterfeit.	**SAE Standards (or other standards, e.g., ERAI or IDEA) will figure prominently, along with other industry standards, in selection among compliant methodologies for this purpose. The new AS 6171 standard establishes a "hierarchy" of test methods, depending on various risk factors – but few companies in the defense supply chain will have the technical means or other resources to conduct all these tests. This suggests some companies will benefit from qualifying test laboratories to have "on call" when risk justifies the cost and time for higher level tests.** **To be considered are costs of different identification methodologies – whether they are chargeable or recoverable – and supply risks if destructive test methods are used. Absent "gold standard" data, it can be impossible to verify the authenticity of older parts or assemblies or to resolve "suspect" status. Prudence dictates not using "suspect" parts and treating such costs as unallowable absent CO approval.**

(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 who flow down the whole -7007 ("system") clause impose on their suppliers corresponding obligations to have compliant systems for all 12 criteria. The mandatory -7008 ("sources") cause does not include the obligation for a "CPDAS " or the 12 crtieria.** **DCMA reviews CPDAS of "covered contractors". Initially, it used a "checklist" approach. DCMA–INST 1205, issued July 2015, employs a risk-based approach with a "counterfeit risk assessment" to determine the "counterfeit risk cause likelihood." High risk contractors are subject to more frequent (and closer) surveillance.** **The "systems" requirement is imposed across a diverse supply chain so is no uniform "answer" to a compliant CPDAS. Also unresolved is whether "covered contractors" are responsible to validate the compliance of their subcontractors or if they can rely upon third-party certification of adherence to Standards. Some use intermediaries such as Exostar to vet the supply chain.**

(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.	**Section 818 and the DFARS apply only to "covered contractors" – about 1,200 companies subject to all of DoD's CAS. Approximately 23,000 companies sell to DoD – and thousands more sell to DoD suppliers. Notwithstanding this language, -7007(e) required flow down of "the substance" of the clause and without language excluding alteration. There is reason to question whether all "covered contractors" in fact flow down the "applicable system criteria". However, the -7008 ("sources") clause is to be included in all subcontracts, including those for commercial items.** **Necessary and reliable supply sources may refuse full flowdown or offer their own measures as surrogates. They will charge more for higher assurance – if they are willing to conform at all. DoD's should interpret and apply the flowdown requirement to allow "covered contractors" to use their low-risk, established sources even where they decline full flowdown. Companies may need to make risk-informed business decisions to retain key suppliers.**

(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.

DoD is especially concerned about cyber-active parts that harbor malicious code or otherwise suffer a software "taint." The 2017 DSB Report, however, found "no DoD system at present collects event information on cyber-physical attacks of electronic components as its primary function."

Conceptually, this is not a particularly difficult, but again experience indicates numerous practical problems. Until *reporting* obligations are clarified and GIDEP is improved, it remains difficult for many actors in industry to know when counterfeits have been found and to integrate source- or parts-risk information into their supply chain planning. The commercial resource, ERAI, operates to collect and distribute info on nonconforming or counterfeit electronics – by P/N, without supplier ID.

The absence of effective systems to collect and disseminate information will impair the ability to learn from "escapes" and frustrate the objective of eliminating counterfeits.

Ultimately, data analytics *should* figure into DoD and industry response. The systems are not now present and the value of such analytics is limited if relevant information is not reported or effectively analyzed and disseminated.

(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.	**See comments above. GIDEP has not materially improved despite the enactment of 818 and promulgation of the DFARS. Reporting practices are inconsistent and dissemination is limited. Industry needs more than just the ability to "screen" reports that happen to be made to GIDEP or to private sources (such as ERAI). However, DoD is taking new initiatives that may improve GIDEP. FAR Case 2013-002 would expand reporting of "Nonconforming Items" but its status is "on hold" pending completion of study of GIDEP improvements. The new DSB Report urges expansion of GIDEP functions, modernization of its technology – and additional funding.** **The value of GIDEP presently suffers presently uncertain obligations on "who," is to report, "what" and "when", etc.**
It is very important to keep informed of reports of counterfeits and to actively seek to scrub both inventory and BOMs to identify reported parts. However, GIDEP has limitations that compromise its utility. There is no assurance that all identified instances of "suspect" or confirmed counterfeit parts are reported to GIDEP and its reports are not validated independently. Membership in GIDEP is limited to US and Canadian companies, and excludes foreign sources.	

(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.

*DoD places **great** emphasis on parts obsolescence. Anticipating and answering this problem involves many functions, beginning with design to avoid vulnerability to OOP or obsolete parts and including proactive supply chain actions years in advance of "end of life" situations.*

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. The value of this 12th criteria is prospective. It does not 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 and unresolved issue is how to treat inventory accumulated before these new rules came in force. The new "sources" clause (-7008(b)(3)(i)(B) requires certain actions where a contractor cannot confirm that a new electronic part "has not been commingled" in supplier inventory". However, treatment of inventory as in the highest risk tier seems unjustified and the obligations – notification, "inspection, testing and authentication", etc. appear to be burdensome.

POLLING SLIDE - 5

What are the hardest issues for you as concern counterfeit electronics parts?

A) Knowing our system complies with DFARS
B) Getting customer to pay for extra assurance
C) Finding parts not available from “trusted sources”
D) Knowing what test and inspection to add, and when
E) Deciding who is to report and when
F) Getting customer direction
G) All of the above

Recap:
Key Implementation Issues
(Aug. 2016 DFARS Revsions)

Recap: I

Subject / Sources of Requirement	Risks	Current Status
Flow Down 246-870-2(a)(2) 246-870-2(b)(2)(ix) 246-870-3(b) 252.246-7007(c)(9) 252.246-7007(e) 252.246-7008(e)	The earlier DFARS required flow down to subcontractors at all levels and there is no exception for COTS or commercial suppliers or small business. But "covered contractors" did 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 refused 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 and how to proceed with sources that object. Flowdown may impose liability risks on suppliers greater than contract value. There was uncertainty as to how to deal with exceptions.	Flowdown is still required. See above. In fact, the -7008 now must be included in all subcontracts, including FAR Pt. 12. Before, contracts with companies below the "covered contractor" threshold would not be subject to a counterfeit clause. The final -7008 clause now recognizes that some suppliers may refuse flowdown. In this case, they fall under "Tier 3" of the hierarchy. They may be used but the contractor is obligated to give notice to the CO. The notification does not require CO approval but the contractor, per 7008(b)(3)(i)(B) , is responsible for inspection, testing and authentication. The same principles apply if inventory is commingled and to "last resort" sources if "nonavailability" excludes lower-risk sources. Some purchasers go beyond the required flowdown to demand that suppliers "guarantee" that no counterfeit will be delivered, assume responsibility for any potential liability and indemnify a purchaser. The revised DFARS requires a contractor [the purchaser] to "assume responsibility for authenticity" where it sources from "contractor-approved suppliers." Such "responsibility" is not equivalent to a "guarantee" of authenticity. It is unreasonable for buyers to demand and for sources to make such a guarantee when moderate or higher risks sources are used – as the DFARS now authorizes.

Recap: II

Subject / Sources of Requirement	Risks	Current Status
Use of suppliers other than the original mfg (now … "in accordance with the clause at 246-870-2(a)(1)(i) 252.246-7007(c)(5) 252.246-7008(b)(1)	DFARS originally expressed 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. Production stoppage or impaired sustainment could result if DFARS were interpreted to prohibit 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. The current "Policy" at 246.870-2(a)(1)(i) states: "(1) Except as provided in paragraph (a)(2) of this section, the Government requires contractors and subcontractors at all tiers, to— (i) Obtain electronic parts that are in production by the original manufacturer or an authorized aftermarket manufacturer or currently available in stock from— (A) The original manufacturers of the parts; (B) Their authorized suppliers; or (C) Suppliers that obtain such parts exclusively from the original manufacturers of the parts or their authorized suppliers; and …"	Much has changed. The DFARS released on Aug. 2, 2016, retains a preference for purchases from original sources. However, the definition of "trusted supplier" is deleted and a new definition is added of "contractor-approved supplier." Implicitly recognizing that parts may not always be available from "trusted suppliers," the DFARS now recognizes three "Tiers" of sources: - Tier 1: corresponds roughly to former "trusted suppliers," e.g., original manufacturers, their authorized suppliers; - Tier 2: where parts not available from (1), 'from suppliers identified by the Contractor as contractor-approved suppliers," provided the contractor uses established industry standards and processes (including inspection, testing and authentication); and that the contractor "assumes responsibility" for such parts and reserving approval right to the CO; or - Tier 3: where a supplier refuses flowdown, obtain parts from sources "other than" those preferred, or where inventory is commingled. Left unresolved, at present are particulars for supplier qualification and criteria for Government review and audit. Reference is made, but only generally, to "established … industry standards and processes." Still, the newly allowed sources represent an important change. It is not always possible to purchase from the OEM (or its authorized distributors) because demand continues for electronic parts that are no longer in production, are obsolete, and/or are no longer stocked by the OEM or its authorized resellers. Contractors remain responsible for the authenticity of parts acquired from lower tier suppliers. Now clarified is that contractors, where parts are not available from "Tier 1", have the legal authority to do purchase from distributors ("Tier 2") – where acting as a "contractor-approved supplier" – or even on a "per part" basis ("Tier 3"). Provided that they have an approved CPDAS, and "follow the rules" as to inspection, testing and authentication, and notification, the costs of replacement and remedy should be allowable.

Recap: III

Subject / Sources of Requirement	Compliance Risk	Business Risk
Legacy Inventory / DFARS Applicability (Preamble) Now: 252.246-7008(b)(3)(i)(B)	The 2014 DFARS Comment indicated that inventory not procured in connection with a previous DoD contract is subject to traceability and authentication requirements. The rule itself was silent on inventory, and the issue arose of 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.	The -7008 rule makes important change. Now, contractors may use inventoried parts even where they "[c]annot confirm that an electronic part is new or previously unused and that it has not been commingled in supplier new production or stock with use, refurbished, reclaimed or returned parts." In this situation – as is true with the parts from "Tier 3" suppliers, the contractor must give notification to the CO. (This can be done for an entire lot.) As to such inventory parts, the contractor also is responsible "for inspection, testing, and authentication, in accordance with existing applicable industry standards" and the contractor must make available documentation (of inspection, testing, and authentication) to the Government upon request. Selection among alternative standards and what level of inspection, test and authentication are not now established.
Traceability 252.246-7007(c)(4) (now "tracking … from the original manufacturer to product acceptance by the Government") 252.246-7008(c)	Supply chain unable to support traceability requirement as originally 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 was provided on what to do (e.g. waiver) where traceability is absent. Contractors were at tisk of disapproval of Contractor Purchasing System. "End to end" traceability has not been the customary, contemporary practice and compliant documentation cannot be created if not existent "upstream" in the supply chain.	DoD continues to emphasize traceability as a strong means to reduce exposure to supply chain tampering. The -7008 (c) clause makes changes to traceability requirements which address some of the problems with earlier demands for traceability – but create others. Where a contractor is not the OEM, it is to have "risk-based process" (taking consequences of failure into consideration) that enable tracking from the OEM to product acceptance by the Government. The feasibility of these instructions and the specifics means of "tracking" are not set. Where the contractor cannot establish this level of traceability, it is (again) "responsible for inspection, testing and authentication" IAW "existing applicable industry standards" – another delegation to the judgment and practices of the contractor. Documentation of traceability and of inspection, testing and authentication must be maintained and made available to the Govt. upon request. The content of traceability information remain unclear as is the relationship between traceability and appropriate inspection, testing and authentication.

Conclusions

- Recent changes to counterfeit parts rules are generally positive.
- But questions remain, e.g.,
  - What methods are acceptable to select "contractor-approved suppliers"?
  - What is required for "inspection, testing and authentication" of parts?
  - How can traceability be implemented with limited purchasing leverage?
  - Can new "tiers" of acceptable suppliers be leveraged for efficiency?
- **CPAD systems based on the 2014 DFARS should be reviewed.**
  - **Many companies use flowdown based upon the 2014 DFARS.**
  - **New sourcing methods and cost rules mean harsh T&Cs are unneeded.**
  - **New processes needed for "Tier 2" supplier and "Tier 3" parts approval.**
- The regs still rely upon manual processes imposed on individual contractors rather than centralized, data-driven systems.
- GIDEP merits funding to modernize information collection and dissemination.

POLLING SLIDE - 6

Where do you think it most important to improve regs on counterfeit electronic parts?

A) Remove requirements for COTS suppliers of parts presently in production

B) Finally produce regs and guidance on qualification of "trustworthy" suppliers

C) Clarify roles / responsibilities of COs and customers

D) Explain what is meant by "risk-based assessment"

E) I don't believe any of this is necessary

About the Presenter: Bob Metzger

This presentation reflects Mr. Metzger's personal views and should not be attributed to any client of his firm or organization with which he is involved or affiliated.

Robert S. Metzger
Rogers Joseph O'Donnell PC
202-777-8951
Rmetzger@rjo.com

Bob heads the Washington, D.C. office of Rogers Joseph O'Donnell, P.C., a boutique law firm that specializes in public procurement matters. He advises leading U.S. and international companies on key key public contract compliance challenges and in strategic business pursuits. Bob is recognized for work on supply chain and cyber security. On these subjects, he has published extensively and has made presentations to many academic, government, industry, legal and technical groups.

Naming him a 2016 "Federal 100" awardee, Federal Computer Week said of Bob: "In 2015, he was at the forefront of the convergence of the supply chain and cybersecurity, and his work continues to influence the strategies of federal entities and companies alike."

Bob is a member of the Defense Science Board Cyber/Supply Chain Task Force that produced the Cyber Supply Chain Study in February 2017. He also is Vice-Chair of the Cyber/Supply Chain Assurance Assurance Committee of the IT Alliance for Public Sector (ITAPS), a unit of the Information Technology Technology Industry Council (ITIC), a prominent trade association.

Bob received his B.A. from Middlebury College and his J.D. from Georgetown University Law Center, where he was an Editor of the *Georgetown Law Journal*. He was a Research Fellow, Center for Science & International Affairs (now "Belfer Center"), Harvard Kennedy School of Government. Bob is a member of the International Institute for Strategic Studies (IISS), London. Academic publications on national security topics include articles in *International Security* and the *Journal of Strategic Studies*.

SUPPLEMENTAL MATERIALS

Section 806 and DFARS 252.239-7008

Interim Rule Nov. 18, 2013

Section 806 of NDAA FY 2012

- Applies to "covered procurement action" where there is a "significant supply chain risk to a covered system"
- A covered procurement involves source selection for a "covered system" or a "covered item of supply"

"Supply Chain Risk"

Section 806(e)(4)

"The term 'supply chain risk' means the risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, **operation**, or maintenance of a covered system so as to surveil, deny, disrupt, or otherwise degrade the function, use or operation of such a system."

An operator of a covered system would be subject to Section 806.

DFARS Subpart 239.73 (Nov. 18, 2013)

"The rule establishes a new provision and clause (see DFARS 239.7306) for inclusion in all solicitations and contracts, including contracts for commercial items or commercial off-the-shelf items involving the development or delivery of any information technology, whether acquired as a service or as a supply, because portions of these contracts may be used to support or link with one or more NSS." 78 Fed. Reg. 69268.

"This rule applies to rule applies to contractors involved in the development or delivery of any information technology, whether acquired by DoD as a service or as a supply." 78 Fed. Reg. 69269.

DFARS Subpart 239.7306: insert the clause, "Notice of Supply Chain Risk," in **all solicitations**, including FAR Part 12, that involve the development or delivery or any IT **whether acquired as a service or as a supply**.

As defined, "information technology" includes equipment "**used by a contractor under a contract with the agency**" where its use is required to perform the service.

"The Contractor shall maintain controls in the provision of supplies and services to the Government to minimize supply chain risk."
DFARS 252.239-7018(b)

FAR: Higher Level Quality Requirements

Higher Level Quality Requirements (Interim Rule)

FAR Case 2012-032
79 Fed. Reg. 70345

Nov. 25, 2014

***FAR* 46.202–4**

Allows agencies to specify and require higher level quality for complex or critical items

PART 46—QUALITY ASSURANCE

■ 3. Revise section 46.202–4 to read as follows:

46.202–4 Higher-level contract quality requirements.

(a) Agencies shall establish procedures for determining when higher-level contract quality requirements are necessary, for determining the risk (both the likelihood and the impact) of nonconformance, and for advising the contracting officer about which higher-level standards should be applied and included in the solicitation and contract. Requiring compliance with higher-level quality standards is necessary in solicitations and contracts for complex or critical items (see 46.203) or when the technical requirements of the contract require—

(1) Control of such things as design, work operations, in-process controls, testing, and inspection; or

(2) Attention to such factors as organization, planning, work instructions, documentation control, and advanced metrology.

(b) Examples of higher-level quality standards include overarching quality management system standards such as ISO 9001, ANSI/ASQC E4, ASME NQA–1, SAE AS9100, SAE AS9003, and ISO/TS 16949, and product or process specific quality standards such as SAE AS5553.

Standards & Best Practices

Role of Standards

Increasingly, both government and industry look to industry standards and best practices to assist in supply chain security.

- **From the government standpoint:**
  - Standards and practices can assist the Government (DoD) in its efforts to reduce the risk of counterfeit electronic parts
  - Standards and practices inform contractors on how to identify and mitigate supply chain risk
  - Emerging supply chain threats (e.g., IoT) call for new standards

- **From industry's standpoint:**
  - Standards act as "reference points" to assure compliance with new government supply chain initiatives
  - Well-developed standards and practices can advance the art and practice of dealing with real-world supply chain events
  - Risk-based assessment and response are promoted

Example: Traceability

JESD243:

- **Supply Chain Traceability (No. 3)** – defined as documented evidence of a part's supply chain history.
- **Return Verification (No. 4.3.2)** – before a manufacturer restocks parts returned to it, it must validate the parts against the traceability records

Critique:

- Beyond definition, no general obligation on device manufacturers to ensure products, once delivered, are traceable either through accompanying documentation or through technical means to verify authenticity.
- Does not serve needs of system purchasers, operators, or maintenance providers

Other Standards:

- **AS 5553A** – must document all supply chain intermediaries and significant handling transactions (i.e., from OCM to distributor; from excess inventory to broker to distributor). Appx. C offers guidance on Supply Chain Traceability. Verification of Purchased / Returned Parts addressed at §4.1.5.
- **AS 9120** –§7.5.3 (Identification and Traceability) details the necessary processes.
- **DLA QSLD** requires documented trail through all Distributors, intermediate possessors, to the specified Approved Manufacturer

JESD243 (JEDEC – Mar. 24, 2016)


COUNTERFEIT MITIGATION

JESD243: An Industry Standard for COUNTERFEIT ELECTRONIC PARTS – or Something Less?

Counterfeit avoidance standards need additional detail for addressing and mitigating key risks.
by ROBERT S. METZGER and MARK NORTHRUP

Circuits Assembly March 2017

Per DFARS -7008, when a contractor cannot establish traceability from the original manufacturer, it must be responsible for "IT&A". JESD's limited treatment of traceability makes it more likely DoD suppliers will receive parts with less documentation that desired, requiring additional inspection, testing and authentication.

Traceability. Under JESD243, supply-chain traceability (No. 3) is defined as documented evidence of a part's supply-chain history. The standard's section on Return Verification (No. 4.3.2) states that before a manufacturer restocks parts returned to it, it must validate the parts against the traceability records.

Beyond the definitions, the standard establishes no general obligation on device manufacturers to ensure products, once delivered, are traceable either through accompanying documentation or through technical means to verify authenticity. Nor does it serve the needs of system purchasers, operators, or maintenance providers.

These limitations are especially unfortunate in light of the August revisions to the counterfeit parts DFARS. The least favored category of sources – the "third tier" – are "other sources" when parts cannot be obtained from the two higher and more trusted tiers. A part can fall into this third tier if a company cannot "confirm" that an electronic part "is new or previously unused and that it has not been comingled in supplier new production or stock with used, refurbished, reclaimed or returned parts." DFARS 252.2467008(b)(3)(i)(B). JESD243 does not impose a positive obligation on a manufacturer to create or maintain documentation sufficient to satisfy the DFARS concern with comingled parts.

The New IPC-1782

- IPC has created a new standard, IPC-1782. (Nov. 1, 2016)
  - At https://www.document-center.com/standards/show/IPC-1782
- IPC-1782 defines four levels for material and process traceability and is designed to apply broadly to products in every company.
- **Subjects addressed include *material* traceability, *process* traceability, *accuracy* (data integrity), *data collection* (automation) and *data retention time.***
- Four levels of traceability are stated, ranging from
  - Level 1 (Basic) (p/n listed to work order, significant process exceptions listed, 90% manual) … to Level 4 (Comprehensive) (unique material ID, all metrics to serialized PCB ass'y, 9 Sigma accuracy, fully automated data collection and storage)
  - Data retention time varies from Life of Product +1 to +7

A Strategic Approach to the Supply Chain

- New technical means are emerging to collect, share and analyze data.
- More industry bodies will be working to develop standards and best practices that align with the emerging traceability technologies.
- Increasingly, companies will use traceability to defend their products and supply chain against the risk of counterfeits of all types.
- While these measures will be “disruptive” of “legacy” traceability approaches, there are great benefits in risk avoidance, brand protection, and regulatory compliance.
- Measures will vary in cost (and protection) and adoption will reflect market considerations and customer requirements.