



Supply Chain Security: DFARS – Detection & Avoidance of Counterfeit Electronic Parts May 11, 2016

Robert S. Metzger
Jeffery M. Chiow
Oliya S. Zamaray

Rogers Joseph O'Donnell, P.C.
875 Fifteenth Street, N.W., Ste 725
Washington, D.C. 20005
(202) 777-8950
www.rjo.com

- Fundamentals:
 - The *threat* of counterfeit electronics
 - The *statute* - Section 818 NDAA FY 2012
 - The *DFARS* – Detection & Avoidance (May 2014)
 - *What* the Rule requires ... *Who* is subject to the Rule ...
How it is implemented
 - Proposed Rules - Sept. 2015 and Mar. 2016
- Policies and Procedures for Compliance
- Advanced Topics:
 - The 12 “System Criteria”
 - Key Implementation Challenges

Why
Laws and Rules to Detect & Avoid
Counterfeit Electronic Parts

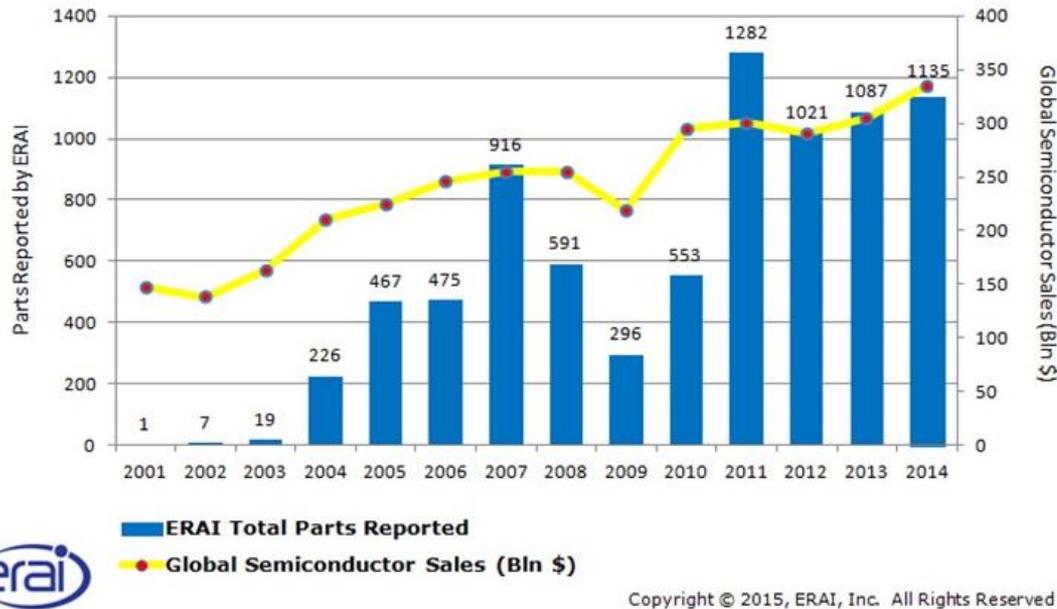
POLLING SLIDE - 1

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!)

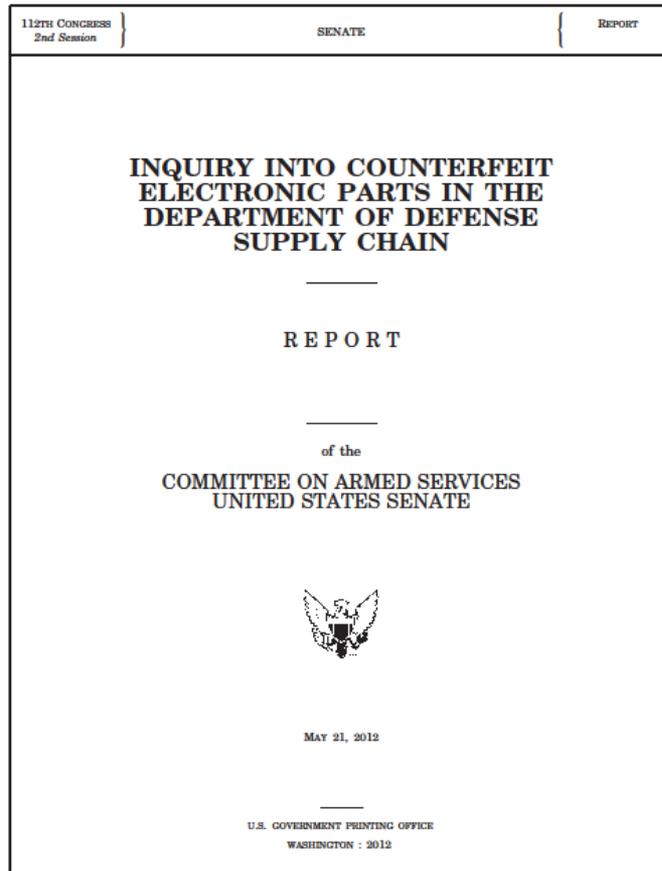
SASC Investigation of Counterfeit Parts

Reported Parts vs. Global Semiconductor Sales



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

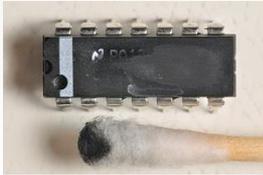


Key SASC findings:

- 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.**

Physical (“Fakes”) vs. Cyber-Physical (“Taints”)

The Ordinary (“Fake”) Counterfeit Part:



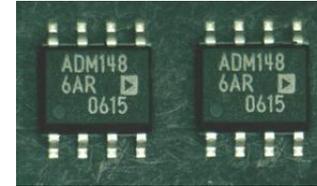
Substandard or non-functional
Likely to fail in intended environment
Presents risk to operations & reliability
Methods exist to detect (in most cases)
Injury :

- 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/>

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

Increased Attention to “Taints”

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

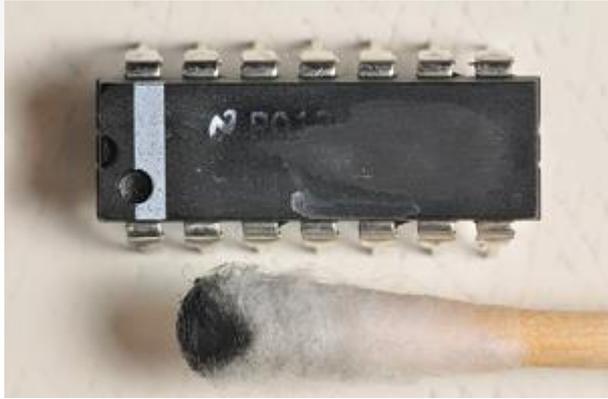
The Result: Section 818 FY 2012 NDAA

Section 818 Operates At Many “Junctions” of the Supply Chain

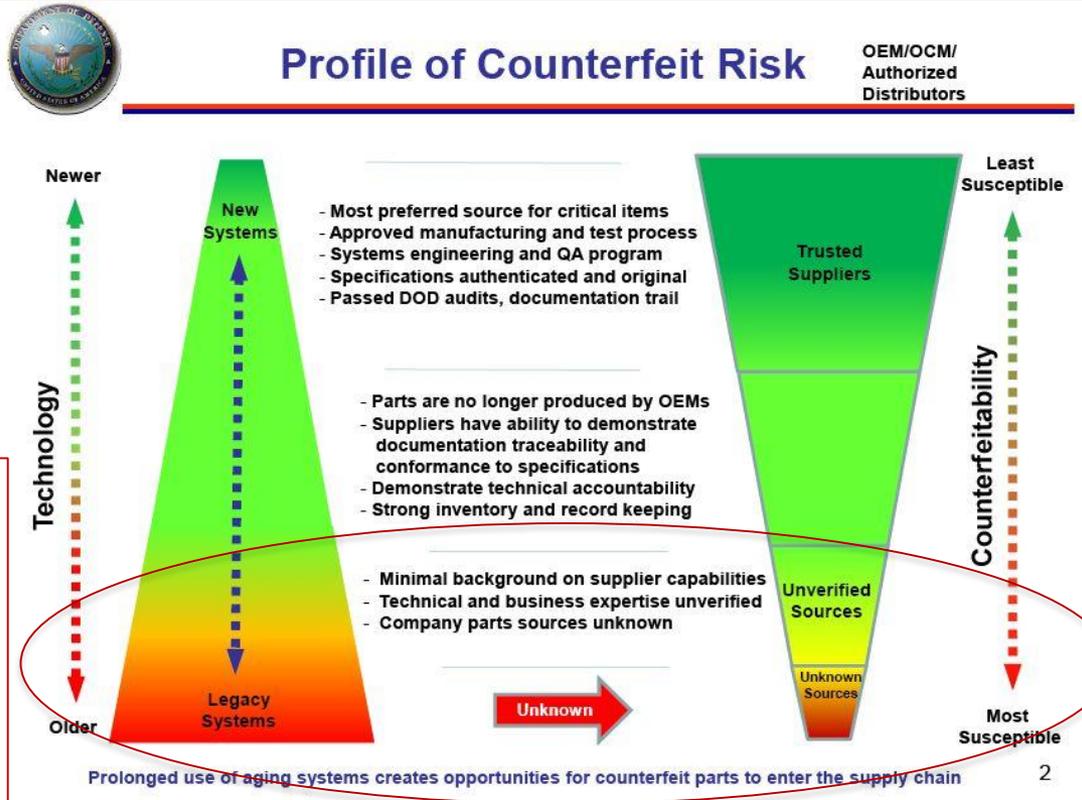
- Detection
- Exclusion
- Enforcement
- **Purchasing Practices**
- **Inspection & Testing**
- **Reporting**
- Corrective Measures
- **Contractor Systems**
- Costs & Incentives
- Sanctions

Section 818 addresses only counterfeit *electronic parts*.
The statute applies only to CAS-covered DoD contractors.
The DFARS regulations require flow down to “all subcontractor tiers”

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

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.

(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.

FINAL RULE: DFARS

Detection & Avoidance of Counterfeit Electronic Parts
79 Fed. Reg. 26092 (May 6, 2014)

DFARS Case 2012–D055

Who is Subject to the DFARS?

The DFARS confirm that Sec. 818 is “specifically limited to **‘covered contractors’**” and that the initial implementation of the rules “has limited application at the prime contract level to CAS-covered contractors.” 79 Fed. Reg. 26098.

However, the flow down requirement causes the rule to affect all subs – including small businesses

The final rule **does exclude set-asides from small business**, because CAS does not apply to small business. “This rule does not apply to small entities as prime contractors.” 79 Fed. Reg. 26105. This limits the **DFARS when DoD purchases from a small business**, as DLA does in high value -- but CAS-covered contractors must flow down.

Promulgation comments recognize that small business subcontractors will incur **“some costs** for complying with prime contractors’ requirements.”

“However, all levels of the supply chain have the potential for introducing counterfeit or suspect-counterfeit electronic items into the end items contracted for under a CAS-covered prime contract. The prime contractor cannot bear all responsibility for preventing the introduction of counterfeit parts. **By flowing down** the prohibitions against counterfeit and suspect counterfeit electronic items and the requirements for systems to detect such parts to all subcontractors that provide electronic parts or assemblies containing electronic parts (without regard to CAS-coverage of the subcontractor), **there will be checks instituted at multiple levels** within the supply chain, reducing the opportunities for counterfeit parts to slip through into end items.” 79 Fed. Reg. 26099.

The Proposed Rule of Sep. 21, 2016 would add a new clause, DFARS 252.246-70XX, that would (i) apply to all businesses, including small business set-asides, and would not be limited to CAS-covered contractors; (ii) allow also use of “trustworthy suppliers” identified by the contractor IAW DoD-adopted counterfeit prevention industry standards and best practices; and (iii) require traceability of parts.

Considerations for Service Providers

Definition of “Electronic Part”

“an integrated circuit, a discrete electronic component (including, but not limited to, a transistor, capacitor, resistor, or diode), or a circuit assembly ... The term “electronic part” includes any embedded software or firmware.”

*The present definition implies **cyber physical security** issues and concerns of tainted hardware – but this is likely to be removed in the next DFARS update.*

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 narrow safeharbor is available] DFARS 231.205-71*

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

Contract Clause

The clause at DFAR 252.246-7007 (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 applies if the contractor is subject to CAS.

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.

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**

Part 202: 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.”*

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**.”*

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 the original manufacturer or an aftermarket manufacturer that has been provided express written authorization from the current design activity or original manufacturer.”*

The Proposed DFAR would remove “embedded software or firmware” from the definition. Why? Because technical methods are not established and there is no accepted industry standard or best practice to determine whether cyber-active electronic parts harbor tampered or defective software or firmware.

Part 231: Contract Cost Principles ...

231.205-71

*“(b) The costs of counterfeit electronic **parts** or **suspect** counterfeit electronic parts and the cost of **rework** or **corrective action** that may be required to **remedy** the use or inclusion of such parts are **unallowable**, unless—*

(1) The contractor has an operational system to detect and avoid counterfeit 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; and

(3) The contractor provides timely (i.e., within 60 days after the contractor becomes aware) notice to the Government.”

- Costs are unallowable for both confirmed and suspect counterfeit parts
- Also unallowable are costs for rework or corrective action to “remedy”
- Measures must be taken to identify, segregate, suspend and/or disallow subject costs
- A very limited “safe harbor” is provided

The Proposed Rule of Mar. 25, 2016 would amend the allowability of costs of counterfeit electronic parts. Costs would be allowable if (a) parts are obtained from trusted suppliers, (b) contractor discovers, and (c) contractor provides timely notice to the Government. Contractor must also be compliant with DFARS 246.870 – System to Detect and Avoid Counterfeit Electronic Parts. If adopted, this change could motivate more counterfeit reporting.

Part 244: Subcontracting Policies & Procedures

244.303 Extent of Review

(b) Also review the adequacy of the contractor's counterfeit electronic part detection and avoidance system under clause 252.246-7007, Contractor Counterfeit Electronic Part Detection and Avoidance System.

244.305-71 Contract Clause

Use the Contractor Purchasing System Administration basic clause or its alternate as follows:

*(a) Use the clause at 252.244-7001, Contractor Purchasing System Administration— **Basic**, in solicitations and contracts containing the clause at FAR 52.244-2, Subcontracts.*

*(b) Use the clause at 252.244-7001, Contractor Purchasing System Administration— **Alternate I**, in solicitations and contracts that contain the clause at 252.246-7007, Contractor Counterfeit Electronic Part Detection and Avoidance System, but do not contain FAR 52.244-2, Subcontracts.*

- Adds counterfeit parts prevention to **Contractor Purchasing System Review**
- The “Basic” clause adds the requirements of a counterfeit part detection and avoidance system to CPSR review criteria
- “Alternate I” imposes purchasing system review criteria that include the requirements of 252.246-7007
- The Part 244 changes may impose **new obligations** on higher tier contractors to **assure that their subcontractors** have systems to detect and avoid counterfeit parts.

The Proposed Rule of Sep. 21, 2016 would add a new clause, DFARS 252.246-70XX, that would apply to all businesses, including small business set-asides, and would not be limited to contractors subject to CAS. This clause would require use of “trusted suppliers” but allow also use of “trustworthy suppliers” identified by the contractor IAW DoD-adopted counterfeit prevention industry standards and best practices. Traceability of parts also would be required – if adopted.

Part 246: Quality Assurance

Adds subpart 246.8: “Contractor Liability for Loss of or Damage to Property of the Government”

246.870 Contractor’ counterfeit electronic part detection and avoidance systems

246.870-1 Scope

(a) Implements section 818(c) of the National Defense Authorization Act for Fiscal Year 2012 (Pub. L. 112–81); and

(b) Prescribes policy and procedures for preventing counterfeit electronic parts and suspect counterfeit electronic parts from entering the supply chain when procuring electronic parts or end items, components, parts, or assemblies that contain electronic parts.

246.870-2 Policy

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

(b) **System criteria.** A counterfeit electronic part detection and avoidance system shall include risk-based policies and procedures that address, **at a minimum**, the following areas (see 252.246–7007, Contractor Counterfeit Electronic Part Detection and Avoidance System):

(System Criteria reviewed below)

Part 252: Solicitation Provision & Contract Clauses

246.870-3 Contract Clause

(a) **Except** as provided in paragraph (b) of this section, use the clause at 252.246–7007, Contractor Counterfeit Electronic Part Detection and Avoidance

System, in solicitations and contracts when procuring—

(1) Electronic parts;

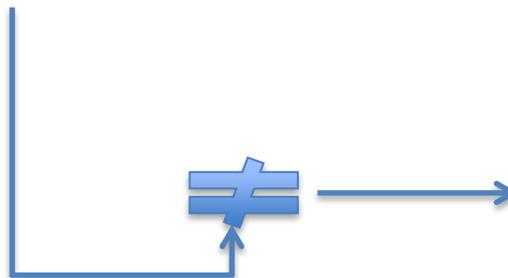
(2) End items, components, parts, or assemblies containing electronic parts; or

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

(b) **Do not use** the clause in solicitations and contracts that are setaside for small business.

- DFARS 252.244–7001 Contractor Purchasing System Administration
- DFARS 252.246–7007 Contractor Counterfeit Electronic Part Detection and Avoidance System

The Proposed Rule of Sep. 21, 2016 adds DFARS 252.246-70XX, that would apply to all businesses, including small business set-asides.



“(e) The Contractor shall include the substance of this clause, including paragraphs (a) through (e), in subcontracts, including subcontracts for commercial items, for electronic parts or assemblies containing electronic parts.”

Section 817 of FY 2015 NDAA

Amends § 818(c)(3) (Trusted Suppliers) to clarify that DoD contractors may obtain electronic parts from authorized dealers “**or from suppliers identified as trusted suppliers**” and “**from alternate suppliers when such parts are not available from original manufacturers, their authorized dealers, or trusted suppliers.**”

DoD regs shall establish qualification requirements by which *DoD may identify as trusted suppliers those that have appropriate policies* and procedures in place to detect and avoid counterfeit electronic parts

And DoD regs shall authorize Department contractors and subcontractors to identify and use “**their own identified trusted suppliers**”

Section 818(c)(3) of the NDAA for FY2012 now reads as follows (emphasis added to highlight changes) ...

(c) Regulations-

(3) TRUSTED SUPPLIERS- The revised regulations issued pursuant to paragraph

(1) shall-

(A) require that 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 **suppliers identified as trusted suppliers in accordance with regulations issued pursuant to subparagraphs (C) and (D);** and who obtain such parts exclusively from the original manufacturers of the parts or their authorized dealers;

(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
(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;**

(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** 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**, 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.

PROPOSED RULE

Detection & Avoidance of Counterfeit Electronic Parts
80 Fed. Reg. 56939 (Sep. 21, 2015)
DFARS Case 2014–D005

Key Provisions



Federal Register / Vol. 80, No. 182 / Monday, September 21, 2015 / Proposed Rules 56943

(a) Partially implements section 818(c) and (e) 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); and
* * * * *

■ 7. Add section 246.870-1 to read as follows:
246.870-1 Definitions.
As used in this section—
Authorized dealer means a supplier with a contractual arrangement with the original manufacturer or current design activity, including an authorized aftermarket manufacturer, to buy, stock, re-package, sell, and distribute its product lines.
Trusted supplier means—
(1) The original manufacturer of a part;
(2) An authorized dealer for the part;
(3) A supplier that obtains the part exclusively from the original component manufacturer of the part or an authorized dealer; or
(4) A supplier that a contractor or subcontractor has identified as a trustworthy supplier, using DoD-adopted counterfeit prevention industry standards and processes, including testing (see <https://assist.dla.mil>).

■ 8. Amend section 246.870-2 by—
■ a. Redesignating paragraphs (a) and (b) as paragraphs (b)(1) and (2), respectively;
■ b. In the newly redesignated paragraph (b)(1), removing the paragraph heading and adding a comma after the second use of “electronic parts”;
■ c. In the newly redesignated paragraph (b)(2), further redesignating paragraphs (1) through (12) as paragraphs (b)(2)(i) through (xii), respectively;

■ d. Adding paragraph (a);
■ e. Adding a paragraph (b) heading;
■ f. In newly redesignated paragraph (b)(2) introductory text, removing “see 252.246-7007” and adding “see the clause at 252.246-7007” in its place; and
■ g. In newly redesignated paragraph (b)(2)(v), adding the phrase “, or use of other trusted suppliers, as identified by the contractor (see paragraph (a)(1)(ii) of this section)” at the end of the sentence, before the period.
The additions read as follows:

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 or currently available in stock from—
(A) The original manufacturers of the parts;
(B) Their authorized dealers; or
(C) Suppliers that obtain such parts exclusively from the original manufacturers of the parts or their authorized dealers;
(ii) Obtain electronic parts that are not in production, or not currently available from stock, from suppliers identified by the contractor or subcontractor as trusted suppliers, provided that—
(A) The contractor uses established counterfeit prevention industry standards and processes, including testing, for identifying such trusted suppliers;
(B) The contractor or subcontractor assumes responsibility for the authenticity of parts provided by such suppliers (see 231.205-71); and
(C) The selection of such trusted suppliers is subject to review and audit by appropriate Department of Defense officials;
(iii) If authorized to purchase electronic parts from the Federal Supply Schedule, contractors and subcontractors are still required to comply with the requirements of paragraph (a)(1) or (2) of this section, as applicable.
(2) If electronic parts are not available from trusted suppliers, the Government requires contractors and subcontractors to comply with the notification, inspection, testing, and authentication requirements of paragraph (c) of the clause at 252.246-70XX, Sources of Electronic Parts.

(b) **Contractor counterfeit electronic part detection and avoidance system.** * * * * *
■ 9. Amend section 246.870-3 by—
■ a. Redesignating paragraphs (a) and (b) as paragraphs (a)(1) and (2), respectively;
■ b. In the newly redesignated paragraph (a)(1), further redesignating paragraphs (1) through (3) as paragraphs (a)(1)(i) through (iii), respectively;
■ c. In newly redesignated paragraph (a)(1), removing “paragraph (b)” and adding “paragraph (a)(2)” in its place;
■ d. In newly redesignated paragraph (a)(1)(iii), removing “Services where” and adding “Services, if” in its place;
■ e. In newly redesignated paragraph (a)(2), removing “set-aside” and adding “set aside” in its place; and
■ f. Adding paragraph (b).
The addition reads as follows:
246.870-3 Contract clause.
* * * * *

(b) Use the clause at 252.246-70XX, 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.

PART 252—SOLICITATION PROVISIONS AND CONTRACT CLAUSES
■ 10. Amend section 252.246-7007 by—
■ a. In the introductory text, removing “246.870-3” and adding “246.870-3(a)” in its place;
■ b. Removing the clause text “(MAY 2014)” and adding “(DATE)” in its place;
■ c. In paragraph (a)—
■ i. Adding, in alphabetical order, the definitions of “Authorized dealer,” “Contract electronics manufacturer,” “Original component manufacturer,” “Original equipment manufacturer,” “Original manufacturer,” and “Trusted supplier”; and
■ ii. Revising the definition of “Electronic part”; and
■ d. Revising paragraphs (c)(4) and (5).
The additions and revisions read as follows:

252.246-7007 Contractor Counterfeit Electronic Part Detection and Avoidance System.
* * * * *
(a) * * * * *
Authorized dealer means a supplier with a contractual arrangement with the original manufacturer or current design activity, including an authorized aftermarket manufacturer, to buy, stock, re-package, sell, and distribute its product lines.
Contract electronics manufacturer means an organization that—
(1) Produces goods, using electronic parts, for other companies on a contract basis under the label or brand name of the other organization; or
(2) Fabricates an electronic part under a contract with, or with the express written authority of, the original component manufacturer based on the original component manufacturer’s designs, formulas, and/or specifications.
Electronic part means 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).
* * * * *
Original component manufacturer means an organization that designs and/or engineers a part and is pursuing, or has obtained, the intellectual property rights to that part.
Original equipment manufacturer means a company that manufactures products that it has designed from purchased components and sells those products under the company’s brand name.
Original manufacturer means the contract electronics manufacturer, the original component manufacturer, or the original equipment manufacturer.
* * * * *
Trusted supplier means—
(1) The original manufacturer of a part;
(2) An authorized dealer for the part;
(3) A supplier that obtains the part exclusively from the original component manufacturer of the part or an authorized dealer; or
(4) A supplier that a contractor or subcontractor has identified as a trustworthy supplier, using DoD-adopted counterfeit prevention industry standards and processes, including testing (see <https://assist.dla.mil>).

(c) * * * * *
(4) Processes to—
(i) 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; and
(ii) If the Contractor cannot establish this traceability from the original manufacturer for a specific part, complete an evaluation that includes consideration of alternative parts or utilization of tests and inspections commensurate with the risk (see paragraph (c)(2) of this clause).
(5) Use of trusted suppliers in accordance with the clause at 252.246-70XX, Sources of Electronic Parts.
* * * * *
■ 11. Add section 252.246-70XX to read as follows:
252.246-70XX Sources of Electronic Parts.
As prescribed in 246.870-3(b), use the following clause:
SOURCES OF ELECTRONIC PARTS (DATE)
(a) **Definitions.** As used in this clause—
Authorized dealer means a supplier with express written authority of a contractual arrangement with the original manufacturer or current design activity, including an authorized aftermarket manufacturer, to buy, stock, re-package, sell, and distribute its product lines.
Contract electronics manufacturer means an organization that—
(1) Produces goods, using electronic parts, for other companies on a contract basis under the label or brand name of the other organization; or
(2) Fabricates an electronic part under a contract with, or with the express written authority of, the original component manufacturer based on the original component manufacturer’s designs, formulas, and/or specifications.
Electronic part means an integrated circuit, a discrete electronic component (including, but not limited to, a transistor, capacitor, resistor, or diode),

56944 Federal Register / Vol. 80, No. 182 / Monday, September 21, 2015 / Proposed Rules

or a circuit assembly (section 818(f)(2) of Pub. L. 112-81).
* * * * *
Original component manufacturer means an organization that designs and/or engineers a part and is pursuing, or has obtained, the intellectual property rights to that part.
Original equipment manufacturer means a company that manufactures products that it has designed from purchased components and sells those products under the company’s brand name.
Original manufacturer means the contract electronics manufacturer, the original component manufacturer, or the original equipment manufacturer.
* * * * *
Trusted supplier means—
(1) The original manufacturer of a part;
(2) An authorized dealer for the part;
(3) A supplier that obtains the part exclusively from the original component manufacturer of the part or an authorized dealer; or
(4) A supplier that a contractor or subcontractor has identified as a trustworthy supplier, using DoD-adopted counterfeit prevention industry standards and processes, including testing (see <https://assist.dla.mil>).

(c) * * * * *
(4) Processes to—
(i) 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; and
(ii) If the Contractor cannot establish this traceability from the original manufacturer for a specific part, complete an evaluation that includes consideration of alternative parts or utilization of tests and inspections commensurate with the risk (see paragraph (c)(2) of this clause).
(5) Use of trusted suppliers in accordance with the clause at 252.246-70XX, Sources of Electronic Parts.
* * * * *
■ 11. Add section 252.246-70XX to read as follows:
252.246-70XX Sources of Electronic Parts.
As prescribed in 246.870-3(b), use the following clause:
SOURCES OF ELECTRONIC PARTS (DATE)
(a) **Definitions.** As used in this clause—
Authorized dealer means a supplier with express written authority of a contractual arrangement with the original manufacturer or current design activity, including an authorized aftermarket manufacturer, to buy, stock, re-package, sell, and distribute its product lines.
Contract electronics manufacturer means an organization that—
(1) Produces goods, using electronic parts, for other companies on a contract basis under the label or brand name of the other organization; or
(2) Fabricates an electronic part under a contract with, or with the express written authority of, the original component manufacturer based on the original component manufacturer’s designs, formulas, and/or specifications.
Electronic part means 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).
* * * * *
Original component manufacturer means an organization that designs and/or engineers a part and is pursuing, or has obtained, the intellectual property rights to that part.
Original equipment manufacturer means a company that manufactures products that it has designed from purchased components and sells those products under the company’s brand name.
Original manufacturer means the contract electronics manufacturer, the original component manufacturer, or the original equipment manufacturer.
* * * * *
Trusted supplier means—
(1) The original manufacturer of a part;
(2) An authorized dealer for the part;
(3) A supplier that obtains the part exclusively from the original component manufacturer of the part or an authorized dealer; or
(4) A supplier that a contractor or subcontractor has identified as a trustworthy supplier, using DoD-adopted counterfeit prevention industry standards and processes, including testing (see <https://assist.dla.mil>).

(c) * * * * *
(4) Processes to—
(i) 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; and
(ii) If the Contractor cannot establish this traceability from the original manufacturer for a specific part, complete an evaluation that includes consideration of alternative parts or utilization of tests and inspections commensurate with the risk (see paragraph (c)(2) of this clause).
(5) Use of trusted suppliers in accordance with the clause at 252.246-70XX, Sources of Electronic Parts.
* * * * *
■ 11. Add section 252.246-70XX to read as follows:
252.246-70XX Sources of Electronic Parts.
As prescribed in 246.870-3(b), use the following clause:
SOURCES OF ELECTRONIC PARTS (DATE)
(a) **Definitions.** As used in this clause—
Authorized dealer means a supplier with express written authority of a contractual arrangement with the original manufacturer or current design activity, including an authorized aftermarket manufacturer, to buy, stock, re-package, sell, and distribute its product lines.
Contract electronics manufacturer means an organization that—
(1) Produces goods, using electronic parts, for other companies on a contract basis under the label or brand name of the other organization; or
(2) Fabricates an electronic part under a contract with, or with the express written authority of, the original component manufacturer based on the original component manufacturer’s designs, formulas, and/or specifications.
Electronic part means 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).
* * * * *
Original component manufacturer means an organization that designs and/or engineers a part and is pursuing, or has obtained, the intellectual property rights to that part.
Original equipment manufacturer means a company that manufactures products that it has designed from purchased components and sells those products under the company’s brand name.
Original manufacturer means the contract electronics manufacturer, the original component manufacturer, or the original equipment manufacturer.
* * * * *
Trusted supplier means—
(1) The original manufacturer of a part;
(2) An authorized dealer for the part;
(3) A supplier that obtains the part exclusively from the original component manufacturer of the part or an authorized dealer; or
(4) A supplier that a contractor or subcontractor has identified as a trustworthy supplier, using DoD-adopted counterfeit prevention industry standards and processes, including testing (see <https://assist.dla.mil>).

Contract electronics manufacturer means an organization that—
(1) Produces goods, using electronic parts, for other companies on a contract basis under the label or brand name of the other organization; or
(2) Fabricates an electronic part under a contract with, or with the express written authority of, the original component manufacturer based on the original component manufacturer’s designs, formulas, and/or specifications.
Electronic part means 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).
Original component manufacturer means an organization that designs and/or engineers a part and is pursuing, or has obtained, the intellectual property rights to that part.
Original equipment manufacturer means a company that manufactures products that it has designed from purchased components and sells those products under the company’s brand name.
Original manufacturer means the contract electronics manufacturer, the original component manufacturer, or the original equipment manufacturer.
* * * * *
Trusted supplier means—
(1) The original manufacturer of a part;
(2) An authorized dealer for the part;
(3) A supplier that obtains the part exclusively from the original component manufacturer of the part or an authorized dealer; or
(4) A supplier that a contractor or subcontractor has identified as a trustworthy supplier, using DoD-adopted counterfeit prevention industry standards and processes, including testing (see <https://assist.dla.mil>).

(c) * * * * *
(4) Processes to—
(i) 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; and
(ii) If the Contractor cannot establish this traceability from the original manufacturer for a specific part, complete an evaluation that includes consideration of alternative parts or utilization of tests and inspections commensurate with the risk (see paragraph (c)(2) of this clause).
(5) Use of trusted suppliers in accordance with the clause at 252.246-70XX, Sources of Electronic Parts.
* * * * *
■ 11. Add section 252.246-70XX to read as follows:
252.246-70XX Sources of Electronic Parts.
As prescribed in 246.870-3(b), use the following clause:
SOURCES OF ELECTRONIC PARTS (DATE)
(a) **Definitions.** As used in this clause—
Authorized dealer means a supplier with express written authority of a contractual arrangement with the original manufacturer or current design activity, including an authorized aftermarket manufacturer, to buy, stock, re-package, sell, and distribute its product lines.
Contract electronics manufacturer means an organization that—
(1) Produces goods, using electronic parts, for other companies on a contract basis under the label or brand name of the other organization; or
(2) Fabricates an electronic part under a contract with, or with the express written authority of, the original component manufacturer based on the original component manufacturer’s designs, formulas, and/or specifications.
Electronic part means 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).
* * * * *
Original component manufacturer means an organization that designs and/or engineers a part and is pursuing, or has obtained, the intellectual property rights to that part.
Original equipment manufacturer means a company that manufactures products that it has designed from purchased components and sells those products under the company’s brand name.
Original manufacturer means the contract electronics manufacturer, the original component manufacturer, or the original equipment manufacturer.
* * * * *
Trusted supplier means—
(1) The original manufacturer of a part;
(2) An authorized dealer for the part;
(3) A supplier that obtains the part exclusively from the original component manufacturer of the part or an authorized dealer; or
(4) A supplier that a contractor or subcontractor has identified as a trustworthy supplier, using DoD-adopted counterfeit prevention industry standards and processes, including testing (see <https://assist.dla.mil>).

(c) * * * * *
(4) Processes to—
(i) 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; and
(ii) If the Contractor cannot establish this traceability from the original manufacturer for a specific part, complete an evaluation that includes consideration of alternative parts or utilization of tests and inspections commensurate with the risk (see paragraph (c)(2) of this clause).
(5) Use of trusted suppliers in accordance with the clause at 252.246-70XX, Sources of Electronic Parts.
* * * * *
■ 11. Add section 252.246-70XX to read as follows:
252.246-70XX Sources of Electronic Parts.
As prescribed in 246.870-3(b), use the following clause:
SOURCES OF ELECTRONIC PARTS (DATE)
(a) **Definitions.** As used in this clause—
Authorized dealer means a supplier with express written authority of a contractual arrangement with the original manufacturer or current design activity, including an authorized aftermarket manufacturer, to buy, stock, re-package, sell, and distribute its product lines.
Contract electronics manufacturer means an organization that—
(1) Produces goods, using electronic parts, for other companies on a contract basis under the label or brand name of the other organization; or
(2) Fabricates an electronic part under a contract with, or with the express written authority of, the original component manufacturer based on the original component manufacturer’s designs, formulas, and/or specifications.
Electronic part means 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).
* * * * *
Original component manufacturer means an organization that designs and/or engineers a part and is pursuing, or has obtained, the intellectual property rights to that part.
Original equipment manufacturer means a company that manufactures products that it has designed from purchased components and sells those products under the company’s brand name.
Original manufacturer means the contract electronics manufacturer, the original component manufacturer, or the original equipment manufacturer.
* * * * *
Trusted supplier means—
(1) The original manufacturer of a part;
(2) An authorized dealer for the part;
(3) A supplier that obtains the part exclusively from the original component manufacturer of the part or an authorized dealer; or
(4) A supplier that a contractor or subcontractor has identified as a trustworthy supplier, using DoD-adopted counterfeit prevention industry standards and processes, including testing (see <https://assist.dla.mil>).

for an electronic part, the Contractor shall have risk-based processes (taking into consideration the consequences of failure of an electronic part) that—
(1) 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; and
(2) If the Contractor cannot establish this traceability from the original manufacturer for a specific part, complete an evaluation that includes consideration of alternative parts or utilization of tests and inspections commensurate with the risk. 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.
(3) **Non-trusted suppliers.** If it is not possible to obtain an electronic part from a trusted supplier, as described in paragraph (b) of this clause, the Contractor shall notify the Contracting Officer. If an entire lot of assemblies require an obsolete component, the Contractor may submit one notification for the entire lot, providing identification of the assemblies containing the parts (e.g., serial numbers).
(2) The Contractor is responsible for inspection, testing, and authentication, in accordance with existing applicable industry standards, of electronic parts obtained from sources other than those described in paragraph (b) of this clause.
(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.
(End of clause)
(FR Doc. 2015-23516 Filed 9-18-15; 8:45 am)
BILLING CODE 5001-06-P

(c) * * * * *
(4) Processes to—
(i) 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; and
(ii) If the Contractor cannot establish this traceability from the original manufacturer for a specific part, complete an evaluation that includes consideration of alternative parts or utilization of tests and inspections commensurate with the risk (see paragraph (c)(2) of this clause).
(5) Use of trusted suppliers in accordance with the clause at 252.246-70XX, Sources of Electronic Parts.
* * * * *
■ 11. Add section 252.246-70XX to read as follows:
252.246-70XX Sources of Electronic Parts.
As prescribed in 246.870-3(b), use the following clause:
SOURCES OF ELECTRONIC PARTS (DATE)
(a) **Definitions.** As used in this clause—
Authorized dealer means a supplier with express written authority of a contractual arrangement with the original manufacturer or current design activity, including an authorized aftermarket manufacturer, to buy, stock, re-package, sell, and distribute its product lines.
Contract electronics manufacturer means an organization that—
(1) Produces goods, using electronic parts, for other companies on a contract basis under the label or brand name of the other organization; or
(2) Fabricates an electronic part under a contract with, or with the express written authority of, the original component manufacturer based on the original component manufacturer’s designs, formulas, and/or specifications.
Electronic part means 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).
* * * * *
Original component manufacturer means an organization that designs and/or engineers a part and is pursuing, or has obtained, the intellectual property rights to that part.
Original equipment manufacturer means a company that manufactures products that it has designed from purchased components and sells those products under the company’s brand name.
Original manufacturer means the contract electronics manufacturer, the original component manufacturer, or the original equipment manufacturer.
* * * * *
Trusted supplier means—
(1) The original manufacturer of a part;
(2) An authorized dealer for the part;
(3) A supplier that obtains the part exclusively from the original component manufacturer of the part or an authorized dealer; or
(4) A supplier that a contractor or subcontractor has identified as a trustworthy supplier, using DoD-adopted counterfeit prevention industry standards and processes, including testing (see <https://assist.dla.mil>).

(c) * * * * *
(4) Processes to—
(i) 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; and
(ii) If the Contractor cannot establish this traceability from the original manufacturer for a specific part, complete an evaluation that includes consideration of alternative parts or utilization of tests and inspections commensurate with the risk (see paragraph (c)(2) of this clause).
(5) Use of trusted suppliers in accordance with the clause at 252.246-70XX, Sources of Electronic Parts.
* * * * *
■ 11. Add section 252.246-70XX to read as follows:
252.246-70XX Sources of Electronic Parts.
As prescribed in 246.870-3(b), use the following clause:
SOURCES OF ELECTRONIC PARTS (DATE)
(a) **Definitions.** As used in this clause—
Authorized dealer means a supplier with express written authority of a contractual arrangement with the original manufacturer or current design activity, including an authorized aftermarket manufacturer, to buy, stock, re-package, sell, and distribute its product lines.
Contract electronics manufacturer means an organization that—
(1) Produces goods, using electronic parts, for other companies on a contract basis under the label or brand name of the other organization; or
(2) Fabricates an electronic part under a contract with, or with the express written authority of, the original component manufacturer based on the original component manufacturer’s designs, formulas, and/or specifications.
Electronic part means 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).
* * * * *
Original component manufacturer means an organization that designs and/or engineers a part and is pursuing, or has obtained, the intellectual property rights to that part.
Original equipment manufacturer means a company that manufactures products that it has designed from purchased components and sells those products under the company’s brand name.
Original manufacturer means the contract electronics manufacturer, the original component manufacturer, or the original equipment manufacturer.
* * * * *
Trusted supplier means—
(1) The original manufacturer of a part;
(2) An authorized dealer for the part;
(3) A supplier that obtains the part exclusively from the original component manufacturer of the part or an authorized dealer; or
(4) A supplier that a contractor or subcontractor has identified as a trustworthy supplier, using DoD-adopted counterfeit prevention industry standards and processes, including testing (see <https://assist.dla.mil>).

DEPARTMENT OF TRANSPORTATION
National Highway Traffic Safety Administration
49 CFR Part 578
[Docket No. NHTSA-2015-0090]
RIN 2127-AL38
Civil Penalty Procedures and Factors
AGENCY: National Highway Traffic Safety Administration (NHTSA), Department of Transportation.
ACTION: Notice of proposed rulemaking (NPRM).
SUMMARY: NHTSA is proposing a rule prescribing procedures for the assessment of civil penalties and for

Features of the Proposed Rule

- Mandates purchase of electronic parts from 4 types of “trusted suppliers”

Original manufacturer (OM)	Supplier that obtains exclusively from the OM or authorized dealer
“Authorized dealer”	“Supplier that a contractor or subcontractor has identified as a trustworthy supplier, using DoD-adopted counterfeit prevention industry standards and processes.”

*Exception when no trusted supplier exists

- Notify the CO and assume responsibility for “inspection, testing, and authentication, in accordance with existing applicable industry standards”
- DoD may someday separately identify trusted suppliers (DFARS Case 2015-D020)
- Clarification regarding “traceability”
 - Non-proscriptive risk-based approach
 - Probability of receiving a counterfeit
 - Probability that inspection or testing will detect counterfeit
 - Potential negative consequences of a counterfeit escape
 - Where traceability cannot be shown, contractor must “complete an evaluation that includes consideration of alternative parts or utilization of test and inspections commensurate with the risk.”

Proposed Rule – Applicability and Scope

Expansions of Applicability and Scope

- Applies to *all* contracts and subcontracts for electronic parts, of any size and at any tier, regardless of CAS coverage
- No small business, commercial or COTS exemption and applies even below simplified acquisition threshold

Important Scope Limitation

- Definition of “electronic part” no longer includes “embedded software or firmware” as industry standards are still under development

PROPOSED RULE
Costs Related to Counterfeit Electronic Parts
81 Fed. Reg. 17055 (Mar. 25, 2016)
DFARS Case 2016–D010

Key Provisions

(a) Partially implements section 818(c) and (c) 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); and

■ 7. Add section 246.870-1 to read as follows:

246.870-1 Definitions.

As used in this section—
Authorized dealer means a supplier with a contractual arrangement with the original manufacturer or current design activity, including an authorized aftermarket manufacturer, to buy, stock, re-package, sell, and distribute its product lines.

Trusted supplier means—
 (1) The original manufacturer of a part;

(2) An authorized dealer for the part;

(3) A supplier that obtains the part exclusively from the original component manufacturer of the part or an authorized dealer; or

(4) A supplier that a contractor or subcontractor has identified as a trustworthy supplier, using DoD-adopted counterfeit prevention industry standards and processes, including testing (see <https://assist.dia.mil>);

■ 8. Amend section 246.870-2 by—
 ■ a. Redesignating paragraphs (a) and (b) as paragraphs (b)(1) and (2), respectively;
 ■ b. In newly redesignated paragraph (b)(1), removing the paragraph heading and adding a comma after the second use of “electronic parts”;

■ c. In the newly redesignated paragraph (b)(2), further redesignating paragraphs (1) through (12) as paragraphs (b)(2)(i) through (xii), respectively;

■ d. Adding a paragraph (b) heading;

■ e. In newly redesignated paragraph (b)(2)(i), removing “(b) (2)(i)” and adding “252.246-7007” in its place; and

■ f. In newly redesignated paragraph (b)(2)(v), adding the phrase “, or use of other trusted suppliers, as identified by the contractor (see paragraph (b) of this section)” at the end of the sentence, before the period.

The additions read as follows:

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 or currently available in stock from—

(A) The original manufacturers of the parts;

(B) Their authorized dealers; or

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

(ii) Obtain electronic parts that are not in production, or not currently available from stock, from suppliers identified by the contractor or subcontractor as trusted suppliers, provided that—

(A) The contractor uses established counterfeit prevention industry standards and processes, including testing, for identifying such trusted suppliers;

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

(C) The selection of such trusted suppliers is subject to review and audit by appropriate Department of Defense officials.

(iii) If authorized to purchase electronic parts from the Federal Supply Schedule, contractors and subcontractors are still required to comply with the requirements of paragraph (a)(1) or (2) of this section, as applicable.

(2) If electronic parts are not available from trusted suppliers, the Government requires contractors and subcontractors to comply with the notification, inspection, testing, and authentication requirements of paragraph (c) of the clause at 252.246-70XX, Sources of Electronic Parts.

(b) *Contractor counterfeit prevention system.*

(1) Amend section 246.870-3 by—
 ■ a. Revising paragraphs (a) and (b) as paragraphs (a)(1) and (2), respectively;

■ b. Adding a paragraph (a) heading; and

■ c. In newly redesignated paragraph (a)(1), removing “paragraph (b)” and adding “paragraph (a)(2)” in its place; and

■ d. Adding paragraph (b).

The addition reads as follows:

246.870-3 Contract clause.

■ 10. Amend section 252.246-7007 by—
 ■ a. In the introductory text, removing “246.870-3” and adding “246.870-3(a)” in its place;

■ b. Removing the clause date “(MAY 2014)” and adding “(DATE)” in its place;

■ c. In paragraph (a)—
 ■ i. Adding, in alphabetical order, the definitions of “Authorized dealer,” “Contract electronics manufacturer,” “Original component manufacturer,” “Original equipment manufacturer,” “Original manufacturer,” and “Trusted supplier”; and

■ ii. Revising the definition of “Electronic part”; and

■ d. Revising paragraphs (c)(4) and (5).
 The additions and revisions read as follows:

(b) Use the clause at 252.246-70XX, 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.

PART 252—SOLICITATION PROVISIONS AND CONTRACT CLAUSES

■ 10. Amend section 252.246-7007 by—

■ a. In the introductory text, removing “246.870-3” and adding “246.870-3(a)” in its place;

■ b. Removing the clause date “(MAY 2014)” and adding “(DATE)” in its place;

■ c. In paragraph (a)—
 ■ i. Adding, in alphabetical order, the definitions of “Authorized dealer,” “Contract electronics manufacturer,” “Original component manufacturer,” “Original equipment manufacturer,” “Original manufacturer,” and “Trusted supplier”; and

■ ii. Revising the definition of “Electronic part”; and

■ d. Revising paragraphs (c)(4) and (5).
 The additions and revisions read as follows:

252.246-7007 Contractor Counterfeit Electronic Part Detection and Avoidance System.

(a) * * *

Authorized dealer means a supplier with a contractual arrangement with the original manufacturer or current design activity, including an authorized aftermarket manufacturer, to buy, stock, re-package, sell, and distribute its product lines.

Contract electronics manufacturer means an organization that—
 (1) Produces goods, using electronic parts, for other companies on a contract basis under the label or brand name of the other organization; or

(2) Fabricates an electronic part under contract with, or with the express written authority of, the original component manufacturer based on the original component manufacturer’s designs, formulas, and/or specifications.

* * * * *

Electronic part means an integrated circuit, a discrete electronic component (including, but not limited to, a transistor, capacitor, resistor, or diode),

implements Section 885(a) of FY 2016 NDAA Proposed Rule depends upon final implementation of DFARS Case 04-D005

- Would expands “safe harbor” for allowable costs, *if*
 - contractor has an DoD-approved system to detect & avoid CEPs; and
 - parts are GFP or were obtained IAW the DFARS 252.246-70XX clause; and
 - contractor discovers the counterfeit or suspect part, and
 - provides “timely (*i.e.*, within 60 days after the contractor becomes aware) notice to the Government.”
- TBD is whether parts from “trusted sources” other than OEMs, e.g., “trustworthy” sources, fall within the “safe harbor.”

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

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.

Goal: mitigate risk to the business and align with DoD's expectations. This is easier said than done, but we've helped companies do it.



Tenets of Effective Counterfeit Part Avoidance & Detection Practices

- **Trust.** Practices should establish a trusted supplier preference, prioritizing purchase of electronic components from OEMs or their authorized distributors.
- **Avoid.** When purchases from suppliers other than the OEM and its authorized distributors are unavoidable, practices should require due diligence to avoid counterfeits .
- **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 11. 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

- **The express requirements of Section 818**
- **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.era.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)

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



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 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.

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 neither established nor common 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 pending **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.

Proposed DFAR: A “trusted supplier” includes a “supplier that a contractor or subcontractor has identified as a trustworthy supplier, using DoD-adopted counterfeit prevention industry standards and processes, including testing.” 246.870–1, 246.870–2 (a)(1)(ii)(A), (a)(2) (where parts “not available from trusted suppliers”). Testing also is to be used, commensurate with risk, where traceability is not present.

(3) Proliferation

Processes to abolish counterfeit parts proliferation.

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 accommodated that such parts may be returned to the supply chain.

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?

(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.

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.

Traceability will improve as new demands become regular practices. But it is not possible to demonstrate traceability “back to the original manufacturer” for many parts and it is not cost-effective or practicable to use only parts with 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. Absence of traceability may indicate additional inspection and test.

E.g., Proposed DFAR: “If the Contractor cannot establish this traceability from the original manufacturer for a specific part, complete an evaluation that includes consideration of alternative parts or utilization of tests and inspections commensurate with the risk (see paragraph (c)(2) of this clause).” 252.246-7007(c)(4)(ii).

(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.

DoD is working on regulations (DFARS Case 2014-D005) to address how covered contractors can be “authorized to identify and use additional trusted suppliers” pursuant to § 817 NDAA 2015. AS-6081 is a useful tool to facilitate purchaser decisions on qualification of distributors.

The core principle of both 818 and the DFARS is 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 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.

Proposed DFAR: “(1) *Non-trusted suppliers.* If it is not possible to obtain an electronic part from a trusted supplier, as described in paragraph (b) of this clause, the Contractor shall notify the Contracting Officer *** (2) The Contractor is responsible for inspection, testing, and authentication, in accordance with existing applicable industry standards, of electronic parts obtained from sources other than those described in paragraph (b) of this clause.” 252.246–70XX (d)

(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.

Reporting is a more complex subject – *but now is an acute problem*. 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. Moreover, some actors 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).

(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.

To be considered are costs of different identification methodologies and supply risks if destructive test methods are used.

(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 industry Standards. **The Proposed DFAR gives additional emphasis to Industry Standards , which figure into purchase from “trusted suppliers” and qualification of “trustworthy suppliers” and into testing of parts.** DoD has adopted AS5553 (Aug. 31, 2009) and AS6081 (Jun. 10, 2013),

The “systems” requirement is imposed across a highly diverse supply chain that produces and supports an enormous breadth of supplies and functions. Many reliable sources decline to accept system elements.

Also unresolved is whether “covered contractors” are responsible to validate the compliance of their subcontractors and if they can rely upon third-party certification of adherence to Standards.

(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. Through flowdown, “covered contractors” are obtain the same anti-counterfeit assurance from all sources in their supply chain – including COTS and commercial sources and small business. 23,000 companies sell to DoD – and thousands more sell to DoD suppliers.

Necessary and reliable supply sources may refuse full flowdown or offer their own measures as surrogates. They will charge more for higher assurance. 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.

Proposed DFAR: “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.” 252.246–70XX(e).

(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.

As progress is made in avoidance of “ordinary” counterfeits, new challenges will arise. The capabilities and sophistication of counterfeiters is increasing, as demand remains for parts in short supply or for lower price. In addition, DoD is especially concerned about cyber-active parts that harbor malicious code or otherwise suffer a software “taint.”

This is not a particularly difficult requirement, conceptually, but again experience suggests there are 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 counterfeit escapes and frustrate the common objective of eliminating counterfeits.

Ultimately, data analytics *should* figure into industry response to the threat of counterfeits – but the value of such analytics is compromised if relevant information is not reported, sufficient nor effectively 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.

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. GIDEP reports are not validated independently. Membership in GIDEP is limited to US and Canadian companies, and excludes foreign sources.

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 to improve GIDEP. This is being done pursuant to FAR Case 2013-002 (Expanded Reporting of Nonconforming Items) (status “on hold” pending completion of study of GIDEP improvements).**

The value of GIDEP presently suffers presently uncertain obligations on “who,” is to report, “what” and “when”, etc.

DoD should promote an automated information exchange that rapidly collects and distributes data on counterfeits. TBD is how to identify and exploit government and private databases (e.g., ERAI), and how to resolve potential inconsistencies in reported info. Ultimately, data analytics should be used to generate and “adjudicate” source risks. Improved standards and methods are needed.

(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. 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.

*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.*

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

Key Implementation Challenges

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 <u>Comment</u> 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 <u>or</u> 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
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.
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 used by DCMA follow 12 System Criteri. 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.

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

Critical Issues

- Flowdown & Supply Chain Assurance
- COTS & Commercial Suppliers
- Protection by Contract
- Treatment of Inventory
- Prime Contractor Obligations
- “Leveraged” Supplier Demo
- Value Chain Diligence
- Pedigree, Provenance & Traceability
- Obsolescence & DMSMS

- “Trustworthy Sources”
- Standards & Best Practices
- Testing & Technical Measures
- Who, When & What to Report
- Responding to “CEP” Events
- Compliance Documentation
- DCMA Oversight
- Potentially Allowable Costs

Summary & Forecast

- Preference for OEMs well-founded – but insufficient
- Sustainment remains a problem – so methods must be approved to qualify other “trustworthy” sources
- Expand “Safe Harbor” to reduce financial exposure
- Reporting patterns have degraded since DFARS
- Expect reinforced and expanded reporting obligations
- DoD at work on improving GIDEP
- Pedigree, Provenance & Traceability are seen as key
- Rules will extend to address taints and malicious code
- Civilian agencies may follow suit (some have)

About the Presenter: Bob Metzger



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

Robert S. Metzger 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 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 government, industry, legal and technical groups, among them ABA (PCL, S&T, SLD), AIA, ASIS, Belfer Center (Harvard), CALCE, CFAM, DoD, DIB SCC, DoJ, DSB, ERAI, Georgetown Law Cyber Institute, IPC, National IPR Center, NCMA, NDIA, SAE, SMTA and SSCA.

Recently named 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. He also is Vice-Chair of the Cyber/Supply Chain Assurance Committee of the IT Alliance for Public Sector (ITAPS), a unit of the Information 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*.

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.

About the Presenter: Jeff Chiow



Jeffery M. Chiow
Rogers Joseph O'Donnell PC
202-777-8952
jchiow@rjo.com

Jeff Chiow is a Shareholder in RJO's Washington office. He focuses on government contracts and government investigations. Jeff is listed among nationally-recognized practitioners by Chambers USA® and as a Rising Star among DC Government Contract Attorneys by Superlawyers®. Mr. Chiow has served clients holding contracts with the Departments of Defense and Homeland Security, every every branch of the military, NASA and intelligence agencies as well as GSA, VA and many other civilian agencies.

Jeff's practice often involves application of creative thinking and foundational procurement principles to unique and emerging issues, especially involving advanced technologies. Recently, he has been called upon to assist clients with difficult questions surrounding the government's growing demands for information assurance, cybersecurity, cloud computing and the transition of legacy IT systems. He has also focused intently on supply chain assurance and the threat posed by counterfeit parts.

Jeff graduated from the U.S. Naval Academy and served as a Marine F/A-18 Weapons and Sensors Officer, serving in the wars in Afghanistan and Iraq, before attending the George Washington University Law School.

Mr. Chiow's comments reflect his personal views and should not be attributed to any client of his firm or organization with which he is involved or affiliated.

About the Presenter: Oliya Zamaray



Oliya S. Zamaray
Rogers Joseph O'Donnell PC
202-777-8953
ozamaray@rjo.com

Oliya is a member of the firm's Government Contracts Group. As part of her practice, Oliya counsels prime contractors and subcontractors on a variety of matters in federal government contracting, including regulatory compliance, subcontract terms and conditions, and procurement integrity issues.

Oliya has experience helping aerospace and defense companies draft policies and procedures to ensure compliance with regulatory regimes governing counterfeit parts, conflict minerals, and domestic sourcing. She has helped government contractors defend against audits and enforcement actions by the U.S. Department of Justice, agency Inspectors General, and agency suspension and debarment officials. Oliya also has helped clients manage internal investigations, has advised on mandatory disclosure rules, and defended against False Claims Act and procurement fraud suits.

Oliya is a 2010 graduate of The George Washington University Law School, where she served as the Senior Notes Editor of the *Public Contract Law Journal*. She obtained her bachelor's degree in Conflict and Security Studies with a minor in Russian language from The George Washington University.

Ms. Zamaray's comments reflect her personal views and should not be attributed to any client of her firm or organization with which she is involved or affiliated.

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.

Risk-Based Analysis (818 DFARS)

$$R = F(T \times V \times C)$$

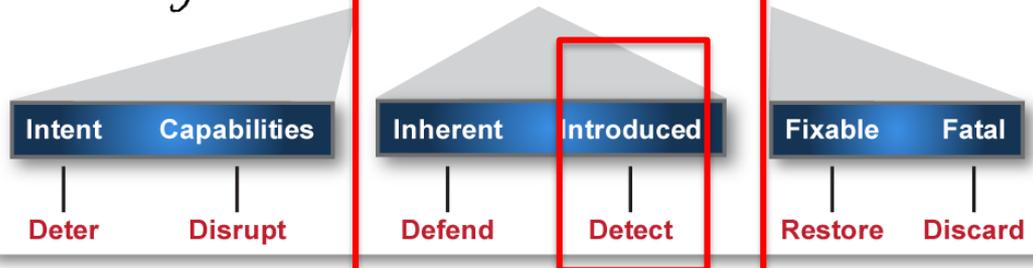
R = Risk

T = Threat

V = Vulnerability

C = Consequence

Risk = f (threat, vulnerabilities, consequences)



DFARS focus

- The DFARS focuses largely on supply chain vulnerability rather than on threats or remediation of consequences.
- Key DFARS attributes are narrowing sources and risk-based test and inspection.
- The DFARS will improve DoD's protection against the "ordinary" counterfeit.
- Different, more rigorous and threat-informed measures will be needed to deal with taints.
- These special methods should focus on mission critical systems and infrastructure.

(DSB Report, *Resilient Military Systems and the Advanced Cyber Threat*, Jan. 2013, at 6)