

An Assessment of the Proposed DFARS Rule on Detection and Avoidance of Counterfeit Electronic Parts (DFARS Case 2012-D055)

Henry Livingston

henry.livingston@ieee.org

INTRODUCTION

The Department of Defense (DoD) is proposing to revise the Defense Federal Acquisition Regulation Supplement (DFARS) to implement, in part, the counterfeit electronic parts prevention requirements described in Section 818 of the National Defense Authorization Act for Fiscal Year 2012 (NDAA2012 §818)¹. While definitive countermeasures can be applied by contractors to manage this problem more effectively, the global nature of the supply chain and current U.S. Government policies, including requirements and exemptions described within the proposed rule, continue to present significant barriers to eliminating counterfeit products from the supply chain altogether. The proposed DFARS rule on “Detection and Avoidance of Counterfeit Electronic Parts”² places responsibility for detecting and avoiding the use or inclusion of counterfeit or suspect counterfeit electronic parts almost exclusively upon large contractors. The proposed rule, however, does not address important issues and leaves a number of gaps unresolved:

Imbalanced Approach to Counterfeit Prevention:

NDAA2012 §818 calls for DoD to implement a risk based approach to counterfeit prevention. The proposed rule, however, does not extend this risk based approach to contractors.

No Criteria established for a “Contractor Counterfeit Electronic Part Avoidance and Detection System”:

The proposed rule requires that contractors have a counterfeit electronic parts avoidance and detection system which the Government must approve but fails to define criteria for an acceptable counterfeit electronic parts avoidance and detection system and also fails to define key terms.

Problematic Definition of ‘Counterfeit Part’:

The definition of “counterfeit part” within the proposed rule introduces a number of inconsistencies and problems.

Missing Definition of ‘Trusted Supplier’:

The proposed rule does not include key elements of a trusted supplier concept specified in NDAA2012 §818.

Parts Obsolescence Issues: The proposed rule fails to address the vulnerability created by continued demand for obsolete parts and fails to address the increasing constraints on DoD regarding its ability to support and fund approaches to eliminate the continued use of obsolete parts needed to support fielded systems and to manufacture new orders to aged, legacy designs and specifications.

Commercial-Off-The-Shelf (COTS) Items: While the DoD has stressed acquisition of commercial items to reduce costs, the proposed rule does not consider the COTS producer’s business practices and its incompatibility with the specific counterfeit parts avoidance methodology described in NDAA2012 §818.

This paper discusses each of these issues and offers the author’s recommendations to address them.

AN IMBALANCED APPROACH TO COUNTERFEIT PREVENTION

NDAA2012 §818 calls for DoD to implement a risk based approach to counterfeit prevention³ and to establish regulations for contractors to “eliminate counterfeit electronic parts from the defense supply chain”⁴. DoD Instruction 4140.67, DoD Counterfeit Prevention Policy⁵, describes a realistic approach to counterfeit prevention. DODI 4140.67 states it is DoD policy to “Not knowingly procure counterfeit materiel” and calls for DoD to “employ a risk based approach to reduce the frequency and impact of counterfeit materiel”. Furthermore, DODI 4140.67 identifies “prevention and early detection” as the “primary strategy in eliminating counterfeit materiel within the DoD”. This strategy is consistent with recommendations the defense industry has communicated to DoD on several occasions over the past few years. Rather than extending this risk based approach to contractors, however, the DoD states in the Discussion section in support of its proposed rule: “*The intent of section 818 is to hold contractors responsible for detecting and avoiding the use...of counterfeit electronic parts...*”⁶ (emphasis added). The strategy implicit within the proposed DFARS rule seeks to address the counterfeit electronic parts threat through: (a) the purchasing systems of prime and upper tier contractors;

(b) DoD approval of these purchasing systems; and (c) the withholding of payments to contractors.

Here are examples of the imbalanced approach to counterfeit prevention described within the proposed DFARS rule on “Detection and Avoidance of Counterfeit Electronic Parts”:

Gaps in Counterfeit Prevention Expectations Throughout the Supply Chain

Counterfeit electronic parts find their way into the supply chain through independent distributors and “brokers”. According to reports published through the Government–Industry Data Exchange Program (GIDEP)⁷, the suppliers associated with the sale of counterfeit electronic parts into the DoD supply chain are independent distributors and brokers. The author analyzed GIDEP Alerts and Problem Advisories on unlimited distribution that document counterfeiting incidents over the past eleven (11) years. In all cases where the specific supplier or category of supplier was identified within these GIDEP reports, the part supplier(s) associated with the sale of suspect counterfeit product was an independent distributor or broker.⁸ The incidents included in the Senate Armed Services Committee (SASC) investigation into counterfeit electronic parts in the DoD supply chain established that they were sold to defense contractors by independent distributors and “brokers”⁹. The proposed rule, however, fails to direct requirements toward these lower tier suppliers.

The proposed DFARS rule introduces a requirement for contractors to “establish and maintain an acceptable counterfeit electronic part avoidance and detection system” as a part of the contractor’s purchasing system. “Failure to do so may result in disapproval of the purchasing system by the contracting officer and/or withholding of payments.”¹⁰ This new requirement, however, will apply only to contracts that are subject to the Cost Accounting Standards (CAS). In other words, the requirements will not apply to any contract less than \$650,000 and will not apply to any contractor which does not have to be CAS-compliant because of its size. According to the Federal Register Notice, “DoD does not expect this proposed rule to have a significant economic impact on a substantial number of small entities ... it applies only to contracts that are subject to the Cost Accounting Standards (CAS) ... Contracts with small entities are exempt from CAS”. Most, if not all, of the suppliers associated with the sale of counterfeit electronic parts described in GIDEP reports and in the SASC report would be exempt from the requirements described in the proposed DFARS rule. Rather than also directing counterfeit prevention requirements toward lower tier suppliers that tend to be associated with the sale of suspect counterfeit electronic parts, the proposed rule focuses on prime and upper tier contractors (large entities subject to CAS) who are not as well positioned to “eliminate counterfeit electronic parts from the defense supply chain”. Prime contractors, for example, are frequently systems architects and systems integrators who may not be involved in the direct

procurement of electronic components; their lower tier suppliers tend to be in a more effective position to implement counterfeit electronic part avoidance and detection practices. According to discussions between the author and numerous defense contractor representatives, many suppliers below the prime and upper tier contractors, however, are reluctant to establish and implement a counterfeit electronic part avoidance and detection system expected of prime and upper tier contractors described in the proposed rule.

Absence of fundamental counterfeit prevention practices and implementation expectations

Counterfeit prevention practices recommended by industry subject matter experts, specified in industry standards, and required of DoD and its contractors per NDAA2012 §818 focus on acquiring electronic parts whenever possible from the most trustworthy suppliers – the original manufacturer or its authorized distributors. DoD’s new counterfeit prevention policy, DODI 4140.67, and the proposed DFARS rule both omit this keystone to counterfeit prevention. Furthermore, the propose rule requires “Contractors’ counterfeit electronic part avoidance and detection systems” to include “Use and qualification of trusted suppliers”, but does not define the term “trusted supplier” or describe expectations or criteria for “use and qualification”. DODI 4140.67 uses a different and broadly defined term – “qualified supplier”. According to DODI 4140.67, ASD(R&E) has been tasked with the responsibility to “[collaborate] with DoD Components to establish technical anti-counterfeit qualification criteria for suppliers”, but there are no expectation of contractors described within DODI 4140.67 and the proposed rule exempts smaller suppliers (including electronic part suppliers) from counterfeit electronic part avoidance and detection requirements to be defined at a future date by ASD(R&E).

“Incentives” for contractors based on inaccurate assumptions of cost recovery

The requirements of the proposed rule concerning unallowable costs are based, in part, on the assumption of Senate Armed Services Committee (SASC) that contractors will recover costs associated with counterfeit part quality escapes from their lower-tier suppliers that provided the counterfeit. In the report of its investigation into counterfeit electronic parts in the DoD supply chain¹¹, SASC asserts that the requirement concerning unallowable costs is intended to “strengthen incentives for contractor adoption of aggressive counterfeit avoidance and detection programs and align DOD contracts with best practices in the commercial sector”. The report refers to examples of DoD contractor standard terms and conditions in support of its conclusion that “Government contracts that permit cost recovery in such circumstances also contrast with agreements contractors enter with their own suppliers.” The SASC report and the proposed DFARS rule do not acknowledge realities that a DoD contractor faces.

The proposed DFARS rule inaccurately presumes: (1) lower level suppliers universally accept counterfeit prevention flow down clauses, and (2) contractors generally recover all costs from its suppliers that supplied counterfeit or suspect counterfeit parts or supplied items containing counterfeit or suspect counterfeit parts. To further complicate matters, smaller suppliers (including electronic part suppliers) who, according to the proposed DFARS rule, would be exempt from counterfeit electronic part avoidance and detection system requirements are not adequately capitalized to be able to hold harmless and indemnify prime and upper tier contractors for costs that cannot be recovered from their customers under NDAA2012 §818.

Recommendations

In order to establish a more balanced DFARS rule on “Detection and Avoidance of Counterfeit Electronic Parts”, DoD should (1) impose a requirement for counterfeit electronic part avoidance and detection systems on contracts and contractors at all tiers, (2) exclude electronic part purchases from small business set asides, and (3) include specific criteria for “counterfeit electronic part avoidance and detection systems” including the central tenets of counterfeit electronic parts prevention¹². ...

- Apply supplier preferences for electronic components purchased from original manufacturers or their authorized distributors,
- Perform due diligence in accordance with recognized industry standards to avoid counterfeits when purchases from sources of supply other than the original component manufacturer and its authorized distribution chain are necessary, and
- Notify government and industry of suspected counterfeits when they are encountered.

To induce the desirable behaviors at all levels of the contractor supply chain, the proposed DFARS rule should incorporate recommendations communicated to DoD in April of 2012 by the Acquisition Reform Working Group (ARWG) on “Refinements to the framework established by Section 818 of the FY 2012 NDAA, Detection and Avoidance of Counterfeit Electronic Parts”¹³:

“... modify subsection (c)(2)(B) as follows:

(c) **REGULATIONS.**—

(2) **CONTRACTOR RESPONSIBILITIES.**— *The revised regulations issued pursuant to paragraph (1) shall provide that –*

(B) *the cost of counterfeit electronic parts and suspect counterfeit electronic parts and the cost of rework or corrective action that may be required to remedy the use or inclusion of such parts are not allowable costs under Department contracts, unless*

(1) *the contractor has a functioning internal operational system for the detection and avoidance of counterfeit parts as required in section 818(e), and*

(2) *the parts were:*

(a) *procured from trusted suppliers per subsection (c)(3) or*

(b) *procured from another source approved by the Department, with additional detection strategies performed per subsection (c)(3), or*

(c) *provided to the contractor as government property per Federal Acquisition Regulation Part 45,*

and

(3) *the contractor provides timely notice to the Government per Section 818 (C)(4).”*

NO CRITERIA ESTABLISHED FOR A “CONTRACTOR COUNTERFEIT ELECTRONIC PART AVOIDANCE AND DETECTION SYSTEM”

A recent article prepared by this author and published by the National Contract Management Association¹⁴ describes how counterfeit parts avoidance and detection has emerged as an area of business and legal risk that aerospace and defense (A&D) contractors should incorporate into compliance programs. The proposed DFARS rule introduces a requirement for contractors to “establish and maintain an acceptable counterfeit electronic part avoidance and detection system”. A contractor’s failure to do so “may result in disapproval of the purchasing system by the contracting officer and/or withholding of payments.” According to the proposed rule, DoD will assess a contractor’s counterfeit electronic parts avoidance and detection system as part of DoD’s contractor purchasing system review (CPSR)¹⁵. The proposed rule, however, fails to define criteria for a contractor’s counterfeit electronic parts avoidance and detection system and DoD has not yet made this criteria available for public comment in advance of implementation.

A number of resources could have been used to specify requirements and implementation details for a contractor's counterfeit electronic parts avoidance and detection system within the proposed rule.

The aerospace and defense industry developed an industry standard for counterfeit electronic parts avoidance, detection, mitigation, and disposition, which includes the central tenets of counterfeit electronic part prevention recommended by industry subject matter experts – SAE Aerospace Standard AS5553¹⁶. This standard was adopted by DoD shortly after its original publication in 2009. AS5553 includes elements of a counterfeit electronic parts control plan that could have been used to articulate requirements and define implementation details within the proposed rule.

NDAA2012 §818 requires the secretary of defense to “implement a program to enhance contractor detection and avoidance of counterfeit electronic parts” and include “processes for the review and approval of contractor systems for the detection and avoidance of counterfeit electronic parts and suspect counterfeit electronic parts.” Section 818(e) of the NDAA 2012 lists several elements that should be addressed within contractor policies and procedures. Though Section 818(e) does not clearly define them, Section 818 (c) provides insight into many of these elements that could have been incorporated into the proposed rule.

The 16 March 2012 memorandum on “Overarching DOD Counterfeit Prevention Guidance”¹⁷ directs specific actions to prevent, detect, remediate, and investigate counterfeiting in the DoD supply chain. The content of this guidance memorandum could have been used to describe an acceptable contractor counterfeit electronic parts avoidance and detection system.

DoD has been evaluating contractor counterfeit detection and avoidance systems based on requirements of NDAA2012 §818 and key industry standards. These evaluations cover purchasing and subcontract management, receiving and inspection, control of nonconforming material, and reporting. The criteria used for these evaluations could have been used to describe an acceptable contractor counterfeit electronic parts avoidance and detection system.

Despite the availability of suitable resources to draw upon, the proposed rule does not define the elements of a contractor's counterfeit electronic parts avoidance and detection system, does not describe criteria for DoD's approval, nor does it include the central tenets of counterfeit electronic part prevention recommended by industry subject matter experts. Instead, the proposed rule includes a list of “system criteria” for a “Contractor Counterfeit Electronic Part Avoidance and Detection System”. These criteria consist of the elements listed section 818(e) of the NDAA 2012:

- The training of personnel.
- The inspection and testing of electronic parts, including criteria for acceptance and rejection. Processes to abolish counterfeit parts proliferation.
- Mechanisms to enable traceability of parts to suppliers.
- Use and qualification of trusted suppliers.
- The reporting of counterfeit electronic parts and suspect counterfeit electronic parts.¹⁸
- The quarantining of counterfeit electronic parts and suspect counterfeit electronic parts.
- Methodologies to identify suspect counterfeit parts and to rapidly determine if a suspect counterfeit part is, in fact, counterfeit.
- The design, operation, and maintenance of systems to detect and avoid counterfeit electronic parts and suspect counterfeit electronic parts.
- The flow down of counterfeit avoidance and detection requirements to subcontractors.

The proposed rule, however, does not define or describe expectations for any of these elements or set forth criteria for system adequacy, nor does the proposed DFARS rule include definitions of key terms.

There is likely a risk for wide disparity among different DoD evaluators in the interpretation of what constitutes an “acceptable contractor counterfeit electronic parts avoidance and detection system.” A number of contractors have already experienced variations in DoD interpretation and evaluations during recent reviews of contractor counterfeit detection and avoidance systems which is largely due to lack of specified, unified criteria on which to base these reviews.

Recommendations

Before DoD proceeds with its implementation of the DFARS rule and its formal assessments, DoD should ...

1. Define the elements of a contractor's counterfeit electronic parts avoidance and detection system, including the central tenets of counterfeit electronic part prevention recommended by industry subject matter experts;
2. Describe explicit criteria for DoD's approval; and
3. Prepare and publish for public comment “Audit Guidance” associated with the assessment and approval of contractor counterfeit electronic parts avoidance and detection systems.

A PROBLEMATIC DEFINITION OF 'COUNTERFEIT PART'

The proposed definition of “counterfeit part” within the proposed DFARS rule introduces a number of inconsistencies and problems.

“Counterfeit part means—

- (1) An unauthorized copy or substitute part that has been identified, marked, and/or altered by a source other than the part’s legally authorized source and has been misrepresented to be from a legally authorized source;
- (2) An item misrepresented to be an authorized item of the legally authorized source; or
- (3) A new, used, outdated, or expired item from a legally authorized source that is misrepresented by any source to the end-user as meeting the performance requirements for the intended use”¹⁹

Inconsistencies

A comparison to the definition found in DoD Instruction 4140.67, DoD Counterfeit Prevention Policy, and in the proposed addition to the NASA FAR Supplement²⁰ reveals a number of inconsistencies.

Subparagraph ‘1’ is nearly identical to the definition within DODI 4140.67. The proposed rule adds the word ‘part’ after ‘substitute’, reinforcing that this proposed rule is confined to ‘electronic parts’ and does not apply to ‘materiel’ in general as DoD specified for its own policy.

Subparagraph ‘1’ in the proposed DFARS rule is also similar to a definition in the proposed addition to the NASA FAR Supplement, but differs with respect to ‘misrepresentation’ (i.e. ‘misrepresented to be from a legally authorized source’ vs. ‘misrepresented to be an authorized item of the legally authorized source’).

Subparagraph ‘1’ also includes the term ‘legally authorized source’ which is also used in DODI 4140.67 and in the proposed addition to the NASA FAR Supplement. The definition of this term within the proposed DFARS rule is identical to that found in the proposed addition to the NASA FAR Supplement. Though used within DODI 4140.67, the term ‘legally authorized source’ is not defined.

Subparagraph ‘2’ is not clear in its distinction from the latter part of ‘1’, but ‘1’ seems to be associated with the supplier of the item, where ‘2’ seems to focus on the item itself. This subparagraph does not appear in the definition within DODI 4140.67 nor does it appear in the proposed addition to the NASA FAR Supplement.

A problematic addition

Subparagraph ‘3’ of the definition of counterfeit part within the proposed DFARS rule is highly problematic. Rather than representing counterfeits as a subset of fraudulent items, subparagraph ‘3’ is very broad and indicates that a nonconforming item that may be wholly unintentional (e.g., a product defect) would be considered counterfeit or suspect counterfeit. This subparagraph does not appear in the definition within DODI 4140.67 nor does it appear in the proposed addition to the NASA FAR Supplement. Here are specific issues I find with subparagraph ‘3’ ...

Misrepresentation: Subparagraph ‘3’ encompasses items “misrepresented by any source to the end-user as meeting the performance requirements for the intended use” which could include an out of spec item due to a temporary lapse of manufacturing and testing process control. Such escapes could well be unintentional and unobserved by the supplier and the product represented to the customer “as meeting the performance requirements for the intended use” which, according to government contract law subject matter experts, could expose the supplier to False Claims Act liability^{21 22}.

New, used, outdated, or expired item: Subparagraph ‘3’ includes “[a] new, used, outdated, or expired item”. While this appears to incorporate the expectations of NDAA2012 §818 to include “previously used parts represented as new” in a Department-wide definition of the term “counterfeit electronic part”, it also includes “outdated” or “expired” items without offering a definition for these terms. Is an obsolete but original part carried in distributor inventory and still in use in fielded products an “outdated” or “expired” item?

Intended use: Subparagraph ‘3’ use of the terms “intended use” and “end-user” could also introduce problems. In the case of an original manufacturer or distributor supplying electronic parts, who determines “intended use”? Would that be the supplier, the contractor that has design application knowledge for the “intended use” for the electronic part, or would that be the DoD “end-user”? A component supplier generally does not know what equipment the electronic part will be used in let alone its “intended use” within that equipment. A component supplier of other than a mil-spec item might argue that the item supplied was not intended for use in military equipment at all. The DoD “end-user” would certainly have knowledge for the “intended use” of the equipment containing the electronic part, but would likely not have design application knowledge for the “intended use” for the electronic part within the design of the equipment.

An omission within the definition of ‘legally authorized source’

The definition of ‘counterfeit part’ within the proposed rule introduces the term ‘legally authorized source.’

“Legally authorized source means the current design activity or the original manufacturer or a supplier authorized by the current design activity or the original manufacturer to produce an item.”²³

The definition of this term, however, does not include ‘authorized distributors’ who are identified as a key element of a trusted supplier concept specified in NDAA2012 §818(c)(3)(A).

Recommendations

Modify the definition of ‘counterfeit part’ within the proposed rule as follows:

Counterfeit part means an unauthorized copy or substitute part that has been identified, marked, and/or altered by a source other than the parts legally authorized source and has been misrepresented to be from a legally authorized source, including previously used parts represented as new.

Modify the definition of ‘legally authorized source’ within the proposed rule as follows:

Legally authorized source means the current design activity or the original manufacturer or a supplier expressly authorized by the current design activity or the original manufacturer to produce or distribute an item.”

MISSING DEFINITION OF ‘TRUSTED SUPPLIER’

The proposed rule does not include key elements of a trusted supplier concept specified in NDAA2012 §818. Referring to Section 818(c)(3)(A), DoD is expected to revise regulations to:

“... 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*;" (emphasis added)

The Federal Register Notice concerning the proposed rule describes partial implementation of NDAA2012 §818, including “the use of trusted suppliers”²⁴. Within its criteria for an acceptable "Contractor Counterfeit Electronic Part Avoidance and Detection System", the proposed DFARS rule

includes “Use and qualification of trusted suppliers”.²⁵ The proposed rule, however, does not include a definition for the term “trusted supplier”, nor does the new DoD counterfeit prevention policy, DODI 4140.67, include a definition for this term.

Section 818(c)(3)(A)(i) includes the keystone to counterfeit avoidance practices recommended by industry and US government subject matter experts and industry standards such as SAE Aerospace Standard AS5553 — use of original manufacturers of the parts or their authorized distributors. It also acknowledges circumstances where one would use other suppliers who, in turn, obtain parts from the original manufacturer or its authorized distributors.

Prior to the release of DODI 4140.67 and the publication of the proposed rule, The Defense Logistics Agency (DLA) introduced the term “trusted source”²⁶ in January 2013 which puts several categories of suppliers on equal footing. This implementation falls short of what NDAA2012§818 requires of DoD and its contractors – apply a strong preference for electronic parts acquired from the original manufacturer or its authorized distributors.

Recommendations

DoD should adopt the keystone to counterfeit prevention within the proposed DFARS rule and within in its own policy. Specifically, DoD should consider the following ...

Develop a definition of the term “trusted supplier” that applies a preference for the use of and original manufacturer or its authorized distributors, and includes suppliers who obtain electronic parts exclusively from the original manufacturer or its authorized distributor.

Adopt definitions within industry standards for the terms “original manufacturer” (e.g. OCM per AS5553) and “authorized distributor” (e.g. “authorized supplier” per AS5553 and “authorized distributor” per proposed AS7777)²⁷.

Include provisions for cases where electronic parts that are not in production or currently available in stock from the original manufacturer or its authorized distributors such that the supplier must apply extra measures to avoid counterfeits. These extra measures must include an assessment of supply chain traceability information associated with the product, and inspections and tests specifically designed to detect and intercept counterfeits.

Should DoD consider including suppliers other than original manufacturers or their authorized distributors as trusted suppliers, develop specific qualification requirements that require these suppliers to apply the extra measures described above when electronic parts are obtained from other than the original manufacturer or its authorized distributors.²⁸

PARTS OBSOLESCENCE ISSUES

Obsolete parts and their relationship to the counterfeit electronic part threat is well known to DoD and its contractors. It has been a prominent topic at various aerospace & defense industry conferences, symposiums, and training programs which have been heavily attended by DoD personnel. This relationship was also discussed in the U.S. Senate Armed Services Committee “Report of the Inquiry into Counterfeit Electronic Parts in the Department of Defense Supply Chain”²⁹. The DFARS proposed rule fails to address the vulnerability created by continued demand for obsolete parts and fails to address the increasing constraints on DoD regarding its ability to support and fund approaches to eliminate the use of obsolete parts.

Defense and aerospace products are particularly vulnerable to counterfeit parts due to part obsolescence. Microelectronics products, in particular, have life cycles far shorter than the defense / aerospace products that use them. When obsolete parts are not eliminated from product designs, and their stocks are not maintained by the original manufacturer and/or its authored distributor. Independent distributors are often used by Government and industry to obtain components that are no longer in production. In order to reduce the likelihood of having to purchase such parts through riskier sources, defense electronics producers and their customers recognize the need to proactively manage the life cycle of electronic products, versus the life cycles of the parts used within them. While requirements within the proposed DFARS rule may reduce the number of purchases from higher risk suppliers, the prominence of through-life support contracts will make part obsolescence a larger challenge and counterfeits a possibly bigger problem for both DoD and defense companies in the future.

Recommendations

The proposed DFARS rule should incorporate recommendations communicated to DoD earlier this year by the Acquisition Reform Working Group (ARWG) on “Refinement of the Framework for the Detection and Avoidance of Counterfeit Electronic Parts”³⁰ :

“Obsolete Parts: the cost of counterfeit electronic parts and suspect counterfeit electronic parts and the cost of rework or corrective action that may be required to remedy the use or inclusion of such parts are not allowable costs under Department contracts, unless:

(1) The contractor’s proposal in response to a DoD solicitation for maintenance, refurbishment or remanufacture work identifies obsolete electronic parts and includes a plan to assure trusted sources of supply for obsolete electronic parts, or to implement design modifications to eliminate obsolete electronic parts; and

(2) DoD elects not to fund design modifications to eliminate obsolete electronic parts; and

(3) The contractor applies inspections and tests intended to detect counterfeit electronic parts when purchasing electronic parts from other than the OEM or its authorized dealer.”

Such approaches will provide the opportunity for DoD and its contractors to establish plans for addressing part obsolescence and to balance the cost of design modifications to eliminate obsolete parts vs. the risk of seeking obsolete parts through riskier sources of supply and the cost to mitigate those risks.

COMMERCIAL-OFF-THE-SHELF (COTS) ITEMS

In its June 2000 report on “Commercial Item Acquisition: Considerations and Lessons Learned”³¹, DoD advises that the use of commercial items “frequently means embracing commercial business practices that are embedded in the commercial item” and “many DoD requirements must be adjusted to accommodate both the vendor’s anticipated uses of the commercial item and the vendor’s business practices”. The proposed DFARS rule, however, fails to address these realities.

In the case of electronic parts, industry and US Government subject matter experts agree that the best way to avoid counterfeits is to buy these electronic parts from the Original Component Manufacturer (OCM) and its authorized distributors. A COTS Original Equipment Manufacturer (OEM) will frequently advise its customers that the best way to avoid counterfeits of its finished products is to purchase them directly from the OEM or its authorized dealer. It is common, however, for the COTS OEM or its authorized dealer to refuse requirements from customers dictating procurement, reporting, and remediation practices such as those described with Section 818 of the FY2012 NDAA. Defense contractors and DoD procurement organizations are frequently faced with a COTS producer’s business practice not to accept such requirements, regardless of what the reality of their procurement, reporting, or remediation practices may be. This is particularly the case of high volume electronics product lines developed for the commercial market, such as IT hardware products, where DoD and its contractors generally do not have the buying power to influence a COTS producer’s business practices for a specific, small volume procurement.

The COTS OEM may list its products on GSA Schedules³² for purchases by all government agencies without the imposition of the requirements described within NDAA2012 §818 or the proposed DFARS rule. Yet, as the proposed clauses are written, the covered contractors would be held liable for the introduction of any suspect counterfeit electronic part into these commercial products if delivered as part of a contractor’s own product or system. In addition, the contractor also faces the risk having its own “Contractor Counterfeit

Electronic Part Avoidance and Detection System” found unacceptable by DoD because the contractor cannot effectively impose the flow down of the proposed DFARS clause on large COTS OEMs.

The proposed DFARS rule introduces a review of contractor subcontracting policies and procedures to include the review of “rationale for documenting commercial item determinations to ensure compliance with the definition of ‘commercial item’ in FAR 2.101” and “the adequacy of the contractor’s counterfeit electronic part avoidance and detection system”. The proposed DFARS rule, however, does not describe the connection between a contractor’s “commercial item determinations” and a contractor’s “counterfeit electronic part avoidance and detection system”, nor does it describe criteria for assessing a contractor’s “commercial item determinations”.

A review of DoD solicitations³³ reveals that some DoD organizations have made adjustments to accommodate the COTS producer’s business practices. Some solicitations require the purchase of COTS products from the OEM or a “Manufacturer Authorized Partner” (consistent with best practice espoused by industry), and require the supplier to “warrant that the products are new, in their original box”. Others call for the supplier to disclose its “counterfeit parts screening procedure and other technical information demonstrating that the supplier can provide the required hardware”. None of these solicitations flow down requirements dictating electronic part procurement, reporting and remediation practices described in NDAA2012 §818 or the proposed rule.

Recommendations

The proposed DFARS rule should squarely address the COTS producer’s business practices and its compatibility with the specific counterfeit parts avoidance methodology described in NDAA2012 §818. Specifically, the following recommendations should be incorporated into the proposed DFARS rule:

- Adopt the practice of purchasing commercially available off-the-shelf products containing electronic parts directly from the OEM or its authorized dealer.
- Exclude from application of clauses described in the proposed rule, whether provided to the US Government under direct purchases or through DoD contracts, those products: (a) purchased from US companies; (b) which are not modified thereafter by the contractor; (c) which the Government confirms would fit the “Commercial Item” definition under FAR 2.101; and (d) which are currently sold on GSA Schedules.
- Include criteria that DoD will use when assessing a contractor’s “commercial item determinations” and

“the adequacy of the contractor’s counterfeit electronic part avoidance and detection system”.

CLOSING REMARKS

This paper described a number of issues gaps associated with the proposed DFARS rule on “Detection and Avoidance of Counterfeit Electronic Parts”. The time table for public comment to this proposed rule will not provide sufficient time and opportunity to engage with key DoD thought leaders and policy makers to hammer out implementation details and criteria for an acceptable contractor counterfeit electronic parts avoidance and detection system. Before DoD proceeds with finalizing the rule and initiates implementation, DoD should collaborate with defense contractors to address implementation issues and gaps such as those identified within this paper.



Henry Livingston is an Engineering Fellow and Technical Director at BAE Systems Electronic Systems. He has published papers on component reliability assessment methods, obsolescence management, semiconductor industry trends and counterfeit electronic components. He is a member of the SAE International G-19 Counterfeit Electronic Parts Committee and major contributor to SAE AS5553; TechAmerica’s Supply Chain Subcommittee; the Industry Advisory Group to the Government-Industry Data Exchange Program; and the IEEE.

~~~~~

*The opinions expressed in this paper are those of the author and do not necessarily reflect the views of BAE Systems Inc., or any of the institutions to which the author is affiliated.*

---

---

## REFERENCES

- <sup>1</sup> H.R.1540 National Defense Authorization Act For Fiscal Year 2012, Public Law No. 112-081, Section 818. Detection and Avoidance of Counterfeit Electronic Parts.
- <sup>2</sup> DARS-2013-0014: Detection and Avoidance of Counterfeit Electronic Parts (DFARS Case 2012-D055)
- <sup>3</sup> NDAA2012 §818 Subsection (b)(2)
- <sup>4</sup> NDAA2012 §818 Subsection (e)(2)(a)
- <sup>5</sup> DoD Instruction 4140.67, DoD Counterfeit Prevention Policy (April 26, 2013)
- <sup>6</sup> Federal Register Vol. 78, No. 95 at p. 28781, II. Discussion
- <sup>7</sup> The Government–Industry Data Exchange Program (GIDEP) is a cooperative activity between government and industry participants seeking to reduce or eliminate expenditures of resources by sharing technical information essential during research, design, development, production and operational phases of the life cycle of systems, facilities and equipment. (<http://www.gidep.org/>)
- <sup>8</sup> The population of GIDEP reports included in this analysis consisted of five-hundred-nineteen (519) Alerts and Problem Advisories discussing one or more counterfeit incidents. The specific supplier or category of supplier was identified in four-hundred-forty (440) of these reports or eighty-five percent (85%) of the population. The oldest report reviewed was published 18 April 2002; the most recent report reviewed was published 4 June 2013. The statistics within this paper is an update of the analysis documented by the author in:  
*Livingston, H., “Observations from Counterfeit Cases Reported Through the Government–Industry Data Exchange Program (GIDEP)”, September 2011.*
- <sup>9</sup> “U.S. Senate Armed Services Committee Hearing to receive testimony on the Committee’s investigation into counterfeit electronic parts in the Department of Defense supply chain”, Nov 2011
- <sup>10</sup> Federal Register Vol. 78, No. 95 at p. 28783, Proposed addition to 48 CFR Part 246—Quality Assurance, subsection 246.870–2
- <sup>11</sup> “Report of the Inquiry into Counterfeit Electronic Parts in the Department of Defense Supply Chain”, Senate Armed Services Committee, 21 May 2012 (112th Congress, 2nd Session, Senate Report 112–167
- <sup>12</sup> Livingston, H., “Compliance Programs for Counterfeit Parts Avoidance and Detection”, Contract Management, National Contract Management Association, May 2013
- <sup>13</sup> 2012 Legislative Recommendations, Acquisition Reform Working Group, April 10, 2013 – Changes to provide exception to strict liability under certain conditions.
- <sup>14</sup> Livingston, H., “Compliance Programs for Counterfeit Parts Avoidance and Detection”, Contract Management, National Contract Management Association, May 2013
- <sup>15</sup> Contractor purchasing system review is “the complete evaluation of a contractor’s purchasing of material and services, subcontracting, and subcontract management from development of the requirement through completion of subcontract performance”. DCMA-INST 143 – Consent to Subcontract (19 March 2013)
- <sup>16</sup> SAE International Aerospace Standard AS5553, “Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition”
- <sup>17</sup> Hon. Frank Kendall, “Overarching DOD Counterfeit Prevention Guidance” (16 March 2012)
- <sup>18</sup> We anticipate this will be described within a forthcoming proposed rule for FAR Case 2013-002, “Expanded Reporting of Nonconforming Supplies”
- <sup>19</sup> Federal Register Vol. 78, No. 95 at p. 28785, Proposed addition to 48 CFR Part 202—Definitions of Words and Terms, subsection 202.101 Definitions: Counterfeit part
- <sup>20</sup> NASA FAR Supplement Regulatory Review No. 1, A Proposed Rule by the National Aeronautics and Space Administration on 04/18/2013, Document Number: 2013-06441
- <sup>21</sup> “DOD Issues Proposed Counterfeiting Rule; Analyst Calls Rule ‘Opaque,’ Too Broad”, Federal Contracts Report, 17 May 2013
- <sup>22</sup> Steven A. Shaw, Mike Wagner, and Robert Nichols “Contractor Responsibility: Toward An Integrated Approach To Legal Risk Management” Briefing Papers © 2013 by Thomson Reuters (March 2013)
- <sup>23</sup> Federal Register Vol. 78, No. 95 at p. 28782, Proposed addition to 48 CFR Part 202—Definitions of Words and Terms, subsection 202.101 Definitions: Legally authorized source
- <sup>24</sup> The use of the term trusted supplier within Section 818 of the FY2012 NDAA differs significantly from its current use with respect to the “DoD Trusted Foundry Program” described within DODI 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN).
- <sup>25</sup> Federal Register Vol. 78, No. 95 at p. 28783, Proposed addition to 48 CFR Part 246—Quality Assurance, subsection 246.870–2 Policy  
Federal Register Vol. 78, No. 95 at p. 28785, Proposed addition to 48 CFR Part 252—Solicitation Provisions and Contract Clauses, subsection 252.246–70XX Electronic Part Avoidance and Detection System.
- <sup>26</sup> DLAD 52.211-9008 Special Notice – Compliance with 52.211-9074, Deoxyribonucleic Acid (DNA) Marking – Federal Supply Class (FSC) 5962 – Trusted Sources.
- <sup>27</sup> The SAE G19 Counterfeit Electronic Parts Committee is developing a new standard, AS7777, which will define the term “authorized distributor”.
- <sup>28</sup> SAE International Aerospace Standard AS6081 includes requirements for use by distributors of electronic parts purchased and sold from the Open Market. While this author has continued concerns that standards, such as AS6081, may focus on the limited abilities of independent distributors rather than on those processes and tests that increase the probability of actual detection of counterfeit parts, the introduction of reasonable national standards would likely result in the reduction of counterfeit parts introduced through this link in the supply chain.
- <sup>29</sup> “Report of the Inquiry into Counterfeit Electronic Parts in the Department of Defense Supply Chain”, Senate Armed Services Committee, 21 May 2012 (112th Congress, 2nd Session, Senate Report 112–167
- <sup>30</sup> 2013 Legislative Recommendations, Acquisition Reform Working Group, 13 March 2013
- <sup>31</sup> “Commercial Item Acquisition: Considerations and Lessons Learned”, 26 June 2000 (<http://www.acq.osd.mil/dpap/Docs/cotsreport.pdf>)
- <sup>32</sup> GSA Advantage!® online shopping and ordering system (<https://www.gsaadvantage.gov/>)
- <sup>33</sup> Examples of solicitations shown in FedBizOps.gov (<https://www.fbo.gov/>) include:  
Solicitation Number: H92257-13-Q-0024, 26 Feb 2013;  
Solicitation Number: HQ0515-3018-0001-000, 15 Feb 2013;  
Solicitation Number: N0017812Q4488, 03 Aug 2012