INSIGHT

Making the Best of the Final DFARS re Counterfeit Parts

By Robert S. Metzger*

Finally, on May 6, 2014 the Department of Defense published a "final rule" to implement Section 818 of the FY 2012 National Defense Authorization Act. This new rule, issued as part of the Defense Acquisition Regulations Supplement (DFARS), is available at 79 Fed. Reg. 26092. Even though it took DoD 2-1/2 years to produce the regulations, the new DFARS deal with only a *part* of Section 818. Other rulemaking efforts are still underway. They will address critical unresolved questions, such as how to qualify suppliers who are not OEMS or authorized distributors. A proposed rule published on June 10, 2014 would expand contractor obligations to report on non-conforming material. DoD officials also have announced that they are drafting rules that will reach even more companies in the federal supply chain, going beyond electronic parts to address counterfeit material and mechanical items.

Waiting for the new DFARS has caused dread among some participants in DoD's supply chain. Higher tier companies worried that the rules would impose costly burdens and liabilities and foreclose their access to necessary out-of-production parts. Those DoD contractors subject to government oversight of "contractor business systems" also were concerned that a counterfeit "escape" would expose their Purchasing Systems to government disapproval, and potentially to reductions in payments. Middle tier companies were troubled that they would be subject to the new rules, where they sell directly to DoD, and also to risk-shifting compliance "flowdown" from their customers who are DoD primes. Companies in the middle tier have no assurance that their downstream supply chain would accept the same anti-counterfeit obligations (and potential liabilities) as may be applied to them. Commercial sources and suppliers of commercial-off-the-shelf (COTS) equipment viewed with great suspicion the prospect that customers who represent only a tiny fraction of their sales might hold them to obligations to meet specialized and costly DFARS requirements. Small businesses, though favored in many defense procurements, faced the uncertain prospect of having to create and maintain costly systems to detect and avoid counterfeit electronic parts. Especially vulnerable were those specialized supply chain participants who answer the continuing demand for out-of-production and obsolete parts. To this group, including stocking distributors, on-demand brokers, and others who use the Internet to match parts supply and demand, the new regulations are a potential threat to business viability because of preferences for purchases from "original" and therefore most trusted sources.

There was something to worry about for virtually every participant in the defense supply chain.

This is not to suggest that participants in the defense supply chain should question the public purpose. Counterfeits pose a very real threat, which runs the gamut from "fakes" created by criminals for their financial gain, to "taints" where adversaries covertly modify authentic parts to impair a military system or execute a cyber attack. Every responsible actor in the defense supply chain should be motivated to improve assurance in the authenticity of its products. Apart from rightly fulfilling customer expectations, anti-counterfeit practices reduce exposure to liability that can result if a counterfeit is delivered and fails. But federal regulations rarely recognize or accommodate the diversity of real world situations and circumstances. Prescriptive regulations could produce unintended and undesired consequences, increase the costs of defense articles, discourage participation in the defense supply base, and potentially disrupt ongoing manufacture and sustainment of military systems.

The final DFARS is not so bad as some feared, but many aspects of its interpretation and application remain as yet unresolved. Some critical issues are essentially ignored, others deferred. The final regulations create new compliance and business risks, the nature of which depends upon where a particular company is placed in the supply chain. Much depends on how the Government will apply and enforce the rules.

At its core, there are several key features to the new DFARS:

1) Contractors subject to the rule (the "covered contractors" – see below) must establish and maintain systems to detect and avoid counter-

INSIGHT

feit electronic parts. The adequacy of these systems will be measured against twelve criteria.

2) An emphasis is placed upon practices that will improve the traceability of electronic parts so that customers are able to know a part's history and chain of custody.
3) DoD will oversee and administer the contractor systems as part of "Contractor Purchasing System Reviews," part of the larger program to monitor "business systems" of larger suppliers.
4) Contractors are strongly encouraged to use original sources (OEMs and OCMs), whenever possible, but are provided no guidance on how they should qualify other sources if needed parts are not available from the sources considered most trusted.
5) Additional test and inspection is required for parts not from the most trusted sources, using "risk-based" methods, though factors and criteria for these methods are not well articulated.
6) Companies must take care to identify both suspect and confirmed counterfeit electronic parts and to give notification when discovered.
7) Costs of replacing counterfeits are unallowable for larger companies that do cost-based contracting with DoD.
8) Suspect and confirmed counterfeit electronic parts must be quarantined and reported to appropriate authorities and measures must be taken to avoid their being returned into the supply chain.
9) Companies are to improve training, make greater use of industry standards and keep informed on reported counterfeit incidents and on new counterfeiting information and trends.
10) DoD contractors subject to the regulation are required to flow down counterfeit detection and avoidance requirements to all levels in the supply chain.

Four critical implementation issues arise from the new rules, as explained below.

Qualification of Additional Trusted Suppliers.

The continuing demand for electronic parts that are no longer available from the original sources creates a problem for contractors subject to the final DFARS. Many parts that are obsolete or no longer in production are available only from independent distributors that happen to hold such parts in inventory, or from brokers, who may find such parts in the open market. Responding to demand for "legacy" parts has been an question since enactment of Section 818. The DFARS regulation was an important opportunity to clarify how DoD and its supply chain should deal with the conflict between statutory insistence upon parts with no counterfeit risk, on the one hand, and market requirements for these parts available only from sources with imperfect assurance, on the other. Unfortunately, the DFARS regulations do no more than acknowledge this critical subject:

> Paragraph (c)(3)(A)(ii) of section 818 also permits the acquisition of electronic parts that are not in production or currently available in stock from trusted suppliers. Paragraphs (c)(3)(C) and (c)(3)(D) require DoD and contractors and subcontractors to establish procedures and criteria for the identification of such trusted suppliers. DoD contemplates further implementation with regard to identification of trusted suppliers under DFARS Case 2014–D005.

79 Fed. Reg. 26095. The rule-makers dropped the ball on this one. No one can deny the active market of demand and supply for parts that cannot be obtained from the "trusted suppliers" as preferred both by Section 818 and the DFARS regulation. All sectors of the supply chain remain unsure whether, in what circumstances, and with what controls they may acquire and use parts from sources, such as distributors or brokers, who are not the original sources.

Although DoD thus far has issued no guidance on this key point, careful analysis shows that the law can accommodate the use of such "additional" trusted suppliers. The plain words of the statute, at section 818 (c)(3), provide that DoD contractors should "*whenever possible*" obtain electronic parts from original manufacturers and their authorized distributors. (Emphasis added.) This phrasing necessarily admits that it may *not* be possible in every situation to acquire parts from these preferred sources.

Section 818(c)(3)(B) requires DoD to "establish requirements for notification" and "inspection, testing and authentication" of electronic parts that are obtained from "any source other than" the preferred categories. Again, the phrasing recognizes that other sources may be utilized.

INSIGHT

DoD should clarify its intentions and offer guidance here, because uncertainty presents a time-sensitive conundrum. Higher tier companies that sustain defense equipment need to purchase parts available only from distributors and brokers. They need to know what rules apply. For their part, distributors and brokers need guidance on what they can or must do to satisfy anti-counterfeit objectives.

In the author's judgment, DoD should confirm that contractors subject to the new DFARS may use their reasonable judgment (risk-informed as appropriate) and make their own decisions on notification, inspection, testing and authentication measures to qualify "additional" trusted suppliers. Where such practices are responsible, guided by industry standards, reflective of historical experience with parts and their suppliers, and documented, contractors should be able to qualify, purchase and use parts from "additional" trusted suppliers that are not OCMs or authorized distributors.

Treatment of Inventory

The focus of Section 818 is on *future* purchases of electronic parts and what measures might be taken to reduce supply chain vulnerability to counterfeits. Neither the statute nor the new DFARS rule say anything about inventory purchased before the new rules. But preliminary regulator Comments that were published along with the DFARS rule have created a major concern for industry.

Responding to a question regarding inventory, one Comment quotes § 818(c)(3)(A)(i) to remind contractors that they are to obtain parts, "whenever possible," that are currently in production or available in stock from the original manufacturer. 79 Fed. Reg. 26095. Another question prompted this answer in the Comments:

> If the parts are already on the contractor's shelf or in inventory, and they were not procured in connection with a previous DoD contract, *they will be subject to the same requirements, such as traceability and authentication*.

79 Red. Reg. at 26099 (emphasis added). Many contractors purchase electronic parts in large quantities and keep them in inventory until required for production or maintenance. Millions of parts have been accumulated. It has not been the common practice to purchase electronic parts to a specific contract or for particular customers, excepting custom items and special parts such as those that are space-qualified. It will not be possible now to impose on parts already in inventory the DFARS' new requirements on "traceability" and "authentication." Retroactive application of these rules is impracticable. In most cases it will be impossible to show the "provenance" of inventory with the same level of data or documentation as will accompany future purchases of electronic parts. Nor is it practicable or affordable to perform tests for "authentication" of all the parts in inventory.

There will be severe and costly consequences unless the new DFARS is interpreted and applied to permit prudent use of accumulated inventory. Companies will be required to discard and replace inventory. Claims may be made against the Government for these costs. Some of the parts now in inventory will be obsolete or otherwise unavailable. That implies disruption to existing manufacturing and support commitments, and the real possibility that companies will be unable to perform existing contracts. What extends this scenario towards the absurd is that this waste – of millions of parts, worth millions of dollars – could occur without any evidence that any parts in inventory actually were flawed, faulty, "suspect" or "counterfeit."

Parts in the inventory of covered contractors should not be presumed to be counterfeit absent some "credible evidence" or, at least, fact-driven indicators or "red flags" to cause additional investigation. Contractors should be authorized to use a "risk-based approach" to assess where (if at all) their existing inventory may be vulnerable to counterfeit insertion, and to determine whether additional authentication or assurance measures are warranted.

The "Flowdown" Contradiction

All companies in the defense supply chain need to understand whether – and how – the new rules apply to them. The statutory source for the new DFARS was Section 818 of NDAA FY 2012. That statute governs *only* the approximately 1,200 DoD contractors (the "covered contractors") who are subject to full or partial coverage of the Cost Accounting Standards (CAS). By some accounts, there are about 13,000 other companies, not subject to CAS, who sell products to DoD. The new rules do *not* apply directly to any of these 13,000 companies or to any companies in their supply chain (unless they happen to be a covered company).

INSIGHT

There can be no doubt, however, that DoD wants all its suppliers, and all their suppliers, to abide by the new rules. The final rule, at DFARS 252.246-7007(c)(9), requires:

> (9) Flowdown of counterfeit detection and avoidance requirements, including applicable system criteria provided herein, to subcontractors at all levels in the supply chain that are responsible for buying or selling electronic parts or assemblies containing electronic parts, or for performing authentication testing.

Despite this demand, DoD knows it lacks the direct legal authority to compel this result. The strategy of DoD's new regulations is to require covered contractors to flow down the anti-counterfeiting requirements to "all levels in the supply chain," including companies responsible for "buying or selling electronic parts or assemblies containing electronic parts." The flowdown would reach commercial and COTS suppliers, and small businesses, regardless of whether they sell directly to DoD.

This is explained in the promulgation Comments:

> 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. at 26009. The rule goes too far in reliance upon an idealized notion of how all tiers of the supply chain will work together. Critically, the rule presumes that covered contractors have sufficient market power to impose the flowdown upon commercial and COTS suppliers. There are many reasons to believe that they do not. Where defense markets are incidental to their business, commercial and COTS suppliers cannot be presumed to accept the costs, burdens and potential liabilities that accompany flowdown of the DFARS. In other cases, OEMs and OCMs will decline to employ DoD-specific anti-counterfeiting measures where they believe their proprietary techniques are superior. Thus, it is virtually guaranteed that flowdown will not occur as the rule-makers sought. Covered contractors, and those below in their supply chain, in many cases will not accept the contractual flowdown.

Even though it is true that risk of counterfeits exists at all tiers and among all classes of suppliers, at least to some degree, companies in the zone where the risk is least will have little incentive to accept the flowdown. DoD may be at greater risk should these suppliers refuse to sell to DoD's covered contractors or should production or support stop because covered contractors cannot get parts from sources willing to accept the flowdown.

By its terms, Section 818 binds only covered contractors subject to CAS, and so the Government can enforce the DFARS regulations only upon such CAS-covered contractors. The promulgation Comments actually confirm that Section 818 is "*specifically limited to 'covered contractors'*" and allowed that the new rule "has limited application at the prime contract level (including implementation of paragraph (c)(3) of section 818 (Trusted Suppliers)) to CAS-covered contractors." 79 Fed. Reg. at 26098 (emphasis added). Thus, the mandatory flowdown, at best, presents a fundamental contradiction because the rule (a) applies only to CAS-covered contractors, but (b) requires flowdown across the entire breadth and depth of a supply chain that is not CAS-covered. It is impossible to reconcile and irresponsible to ignore this discrepancy, and the desired 100% flowdown will not be achievable in the marketplace.

Companies that are not CAS-covered become subject to Section 818 or the DFARS regulations *only to the extent* they accept the flow-down in a contract term from a covered contractor. It both unreasonable and unnecessary to expect that all companies in the defense supply chain will accept full flowdown. Companies should be encouraged to improve their anti-counterfeit practices, but not excluded from DoD's industrial base if they choose not to accept the full DFARS flowdown.

For the same reasons, the DFARS rule makes a serious error by putting *covered* contractors at risk for disapproval of their Purchasing System, or for some other form of non-compliance should their vendor

INSIGHT

base decline to accept the flow-down or insist upon different terms to vary the obligations and risks.

Surely DoD does not intend that its covered contractors will apply for waivers or other specific relief each time that a member of their supply chain refuses to accept the flowdown or negotiates a different deal. That result would be absurd and highly disruptive to the industrial base, to the system of defense supply and support and to contract administration. Accordingly, DoD must issue guidance to recognize that a contractor's system will not fail Contractor Purchasing System Review (CPSR) where contractors find they must continue to do business with suppliers who will not accept the flow-down or insist upon modified application.

Flexible Administration

A contractor's counterfeit parts prevention system must address twelve system criteria. DFARS 246.870 -2(b)(1) - (12). For three of these – training, traceability and methodologies to identify suspect counterfeit electronic parts – the promulgation Comments expressly assert that the rule provides a contractor with "*flexibility*." See DFARS 246.870-2(b)(1), (b)(4) and (b)(7).

- For training, the Comments state that "DoD is providing contractors with the flexibility to determine the appropriate type of training required for individual firms." 79 Fed. Reg. at 26097.

- For traceability, the Comments advise that the rule "provides a contractor flexibility to utilize industry standards and best practices to achieve the required outcome." 79 Fed. Reg. at 26097.

- Similarly, as concerns the methodologies to identify "suspect" parts, the Comments indicate that "the rule provides the contractor flexibility to employ a risk-based approach to tests and inspections." 79 Fed. Reg. at 26098).

By reference to flexibility for three system criteria, DoD recognizes that implementation of the rule must be context-driven because the universe of affected companies is so diverse. Industry wonders, however, whether flexibility also will govern oversight and administration of the nine other required system elements. Some of these appear relatively straightforward, but in actual implementation there will be great variety as covered contractors seek to adapt the rule to their business. The nine other categories – where flexibility also is needed – are inspection and testing of electronic parts (#2), processes to abolish counterfeit parts proliferation (# 3), use of suppliers that are the original manufacturer (#5), reporting and quarantining (#6), design, operation and maintenance of systems to detect and avoid counterfeit electronic parts (#8), flowdown (#9), keeping informed of information and trends (#10), screening GIDEP reports and other sources (#11), and control over obsolete parts (#12).

Oversight authorities, principally DCMA, should refrain from any attempt to prescribe "one size fits all" solutions for any of these. Contractors should be encouraged to demonstrate how they answer the demands of the law and the new DFARS and why their solutions are reasonable in light of their business requirements and the risk relevant to their sources of supply and their products. DCMA should strive to share what it learns of best practices and decisions it makes on implementation. DCMA also should be careful to recognize, especially for larger contractors, the importance of consistency in administration across business units and over time.

DCMA should always be heedful of the tension between the costs of compliance, the disruption to sources of supply and sustainment, and the actual benefits realized in avoidance of counterfeit electronic parts. While all responsible parties seek to reduce the exposure of the defense supply chain to counterfeit electronic parts, that does not mean that companies can be held to impossible standards, impracticable practices or unaffordable costs.

Robert S. Metzger is a shareholder with the law firm of Rogers Joseph O'Donnell and is the Managing Partner of its office in Washington, D.C., a Vice-Chair of TechAmerica's Supply Chain Assurance Subcommittee and a widely published and cited author on counterfeit parts avoidance and related cyber security matters. He can be reached at rmetzger@rjo.com or by phone at (202) 777-8951.