Avoiding Counterfeit Electronic Parts: How DoD's Proposed Rule May Affect You

By
Robert S. Metzger*
Rogers Joseph O'Donnell, PC

On September 21, 2015, DoD published a Proposed Rule to modify its existing regulations on detection and avoidance of counterfeit electronic parts. 80 Fed. Reg. 56939. DoD held a public meeting to get input on the proposed rule on November 13, 2015. By action taken on October 21, 2015, DoD extended the comment period until December 11, 2015. 80 Fed. Reg. 63735. For information on how to submit comments, see http://www.gpo.gov/fdsys/pkg/FR-2015-10-21/pdf/2015-26749.pdf.

For smaller companies, the most important changes in the Proposed Rule are in a new contract clause, presently named DFARS 252.246-70XX ("Sources of Electronic Parts"), that Department of Defense purchasing activities are to use 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. Small business set-asides are subject to the rule.

Before, the regulations covering counterfeit electronics required larger DoD contractors – namely, companies whose DoD contract revenues are large enough to make them subject to Cost Accounting Standards requirements – to have systems and procedures to detect and avoid counterfeit electronic parts. These companies were under a flow-down obligation, so some smaller vendors who support the big defense contractors already have seen their customers include solicitation requirements and special terms and conditions that to reduce the risk of counterfeit parts on purchases intended for DoD customers. Before, however, there was no mandatory DFARS clause that would apply to all solicitations and that would mandate specific measures on the part of the entire supply chain.

These rules follow enactment of Section 818 of the NDAA for FY 2012, following Senate hearings that revealed the danger of counterfeit electronic parts. DoD is especially vulnerable because many of its fielded systems were built and deployed years or even decades ago. That makes it hard to support this

---

* Bob Metzger heads the Washington, D.C. office of Rogers Joseph O'Donnell, PC, a boutique law firm that has specialized in public procurement matters for more than 30 years. Bob is a nationally recognized expert in cyber and supply chain security, with numerous presentations and publications to his credit. Many of these are available at http://www.rjo.com/pub_counterfeit.html.

equipment, because parts needed for sustainment all too often cannot be found through "trusted sources" such as original manufacturers or their authorized distributors. Unscrupulous parties have exploited the continuous demand for these parts though they may be obsolescent and out of production for years. Following enactment of Section 818, DoD published the final DFARS rule, on May 9, 2014, 78 Fed. Reg. 26092, that is the subject of the proposed revision.

DoD systems draw upon an *enormous* and diverse supply chain. In fact, the promulgation comments accompanying the proposed rule indicate that DoD estimates the rule will apply to approximately *33,000* small entities that have DoD prime contracts or subcontracts or who supply electronic parts or components to or for DoD customers. DoD and its higher tier suppliers will continue to buy and sometimes favor purchases from small business, who may react negatively to the obligations, costs and compliance risks of the proposed counterfeit rule. Similarly, DoD continues to purchase electronic parts from commercial and COTS suppliers who may react to this rule as unnecessary, intrusive and asking them to incur special costs to accommodate a particularly demanding customer – the Pentagon – who represents a very small part of their markets.

Before you reach a judgment about the proposed rule, let's consider briefly the context and the reasoning behind the extension to smaller business, commercial and COTS suppliers. Simply put, if a counterfeit electronic part is installed in a weapon system, such as a combat aircraft, when it fails there will be hazard to the flight crew and likely mission failure. The Senate's lengthy hearings and many other sources confirm that there are many sources around the world all too ready and sometimes quite capable of selling fakes that only seem genuine. Vulnerability exists because of the continuing demand for old parts that trusted sources don't have. The consequences of a counterfeit can be severe.

It makes no difference, in terms of the consequence of a counterfeit part that fails, if it comes from a big DoD prime or a small business vendor many tiers below. In fact, there is some reason to think that vulnerability to counterfeit parts is greater as you move "down" the supply chain to smaller and less sophisticated companies, because they are less likely to have the systems and procedures, or the test and inspection capabilities, to readily defend against this threat.

So in the view of this observer, DoD has very good reasons to impose the counterfeit avoidance rule on the whole of its supply chain. Those reasons, however, don't make the rule practicable and don't inform companies newly subject to the rule of what they are supposed to do. Nor do they answer the question of whether these new obligations are affordable.

The commercial part of the DoD supply chain should recognize the risk of counterfeits, but that risk does not apply equally to all commercial or COTS suppliers. A central premise of DoD's regulatory scheme is that larger contractors covered by the full rule should employ risk-based analysis to assess whether a particular transaction from a specific supplier for an identified electronic part carries unacceptable risks, or, perhaps, higher than ideal risks which indicate that test and inspection should be done for risk mitigation.

Applying this principle, there is low risk in purchases from established commercial and COTS suppliers who are furnishing parts that are currently in production. Additional confidence can be gained if such

suppliers keep good records and, especially, where they are willing issue a "certificate of conformance" to document authenticity. "Pedigree" is the word applied to verify that the source of a purchased part is the party authorized to make or sell it. "Provenance" applies to the process after delivery by which parts are transferred, warehoused, distributed and eventually sold. Good documentation of both "pedigree" and "provenance" is referred to as "traceability" – an objective of both the original and the proposed rule. Traceability is an important prospective objective, but DoD should not expect its supply chain to invent documentation for historical purchases when the rules and expectations were different.

Compliance is more difficult for small businesses who may be called upon to acquire, install and sell equipment that has electronic parts they cannot obtain from those original, "trusted" sources. It is important for their higher tier customers, namely the defense primes who are fully covered by the counterfeit rule, to help their small business partners with compliance. This means making technical expertise and resources, including testing, available. In my opinion, through "mentoring" and cooperative engagement of challenges posed by the rule (if adopted as proposed), primes can fulfill their obligations to the Pentagon and help ease the burden and reduce the risk of noncompliance by their small business suppliers.

From a contractual standpoint, some primes have a penchant to take a DFARS obligation applied fully to them and then to demand literal compliance by all their subs at every level as a condition to continue to remain an acceptable supplier. I do not believe that primes must or should attempt to push down all the duties, risks and liabilities to their smaller vendors. They can fulfill the intent of the rule with prudent, risk-based, cooperative measures, and when necessary by seeking guidance or even approval from the government purchasing activity. It certainly would help, however, for the drafters of the DFARS to improve the rule to better inform smaller companies, COTS and commercial suppliers of what is expected of them. DoD can work with the SBA, for example, to make special support resources available. In addition, DoD should issue implementation instructions, for its contracting and oversight personnel, in the form of Procedures, Guidance and Information (PGI) and FAQs, to answer the recurring questions, dispel myths and better inform its huge industrial base of how to make this work.

Let's conclude with a brief examination of the specifics of the proposed new 252.246-70XX clause. Some of it is fairly straightforward. Other aspects make good business and engineering sense. The *fundamental* feature of the proposed clause is that contractors should narrow their sources of electronic parts to reduce buys from potentially untrustworthy sources. Buying parts that are in production or currently in stock from the original source or authorized dealers and suppliers is the best way to fulfill this objective. If needed parts can't be obtained from this preferred class, resort should be made to other suppliers – who may include companies qualified to act as "distributors" of hard to obtain parts – provided that certain controls are applied. First, a small business may be able to utilize distributors qualified by their customer as "trustworthy." (This is to be done by reference to a number of new industry standards and best practices. A small number of distributors have gone to great lengths and costs to establish their credentials and capabilities in counterfeit parts avoidance.) Another hedge is to arrange for test and inspection parts of at-risk parts. If a company doesn't have these abilities in house, it can ask its higher tier customer for its recommendation(s), or it can hire third party resources for this function. (Care should be taken to verify the claimed capabilities of the test and inspection resource.)

Another clause in the proposed rule is problematic and should be clarified. It states, as another condition of a contractor using a part from other than the most trusted sources, that the "Contractor" (sic) "assumes responsibility for the authenticity of parts" that it may obtain from sources of lesser assurance. I read this clause as applicable directly to the supplier who enters into a prime contract with DoD that makes it (the "Contractor") obligated to flow down the clause requirements in its subcontracts and purchase orders. I *also* believe that the correct interpretation is that DoD intends that its direct supplier – the "Contractor" that is in privity with DOD – bears the responsibility for authenticity. But there is some ambiguity as to who is the "Contractor" with this obligation. I do not see it as necessary, reasonable or (in most cases) as even plausible for downstream vendors to assume this responsibility. That is too much risk, with too many of the functions driving the risk outside the vendor's control. My take is that vendors should act responsibly, assess their vulnerability to counterfeits and improve their processes to reduce these risks. In dealing with particular parts, vendors should consult available industry standards and best practices. They should seek guidance and instruction from their customers, and from DoD or SBA if the resources are available. But they need not and must not be made the "guarantors" of the authenticity of electronic parts which they can purchase only from less than "trusted suppliers.

Price comes into this equation as well. Too often, lowest price has been a principal motivation of government customers who purchase supplies and support for legacy systems. This must change. Higher supply chain assurance is not free. The objectives of the counterfeit parts rule – which I consider to be important and generally well-considered – cannot be achieved without a change in *purchaser* practices and receipt of necessary funding to pay for higher assurance. The same principle applies to prime and higher tier customers.

There are other facets and features of the proposed rule and many strategies that can be considered to assure compliance, retain and even grow business in the defense supply chain. My team would be pleased to consult.