Bloomberg BNA

Federal Contracts Report™

Counterfeit Parts

View From RJO: A Standards-Based Way To Avoid Counterfeit Electronic Parts

BY ROBERT S. METZGER

Nearly three years ago, Congress enacted the FY 2012 National Defense Authorization Act (NDAA) that contains Section 818, addressing detection and avoidance of counterfeit electronic parts. The Final Rule on DFARS Case No. 2012-D055 was published six months ago, on May 6, 2014. 79 Fed. Reg. 26092. The regulations affect six subparts of the DFARS. Changes to Part 244 (Subcontracting Policies and Procedures) add counterfeit parts prevention to subjects included in Contractor Purchasing System Reviews (CPSRs). Changes to Part 246 (Quality Assurance) add a new subpart 246.8 that obligates contractors *and their subcontractors* to establish and maintain an ''acceptable counterfeit electronic part detection and avoidance system.'' DFARS 246.870-2 (emphasis added). Failure to do so may result in disapproval of the purchasing system and/or withholding of payments. According to the ''system criteria'' a counterfeit avoidance system shall include ''risk-based policies and procedures'' that address, ''at a minimum,'' twelve criteria contained in the contract clause at DFARS 252.246-7007.

Robert S. Metzger is the head of the Washington, D.C. office of Rogers Joseph O'Donnell, P.C. RJO has focused on public contracts matters for more than 30 years. Mr. Metzger has written extensively on supply chain assurance. He is the Vice-Chair of the Software and Supply Chain Assurance Working Group of the IT Alliance for Public Sector (ITAPS), a unit of the Information Technology Industry Council (ITIC).

Formally, Section 818 and the new DFARS apply only to the approximately 1,200 DoD contractors that are subject to the Cost Accounting Standards (CAS). But the regulations impact many more companies in the supply chain – even beyond the 23,000 other companies that sell to DoD but are not large enough to be CAS-covered. This is by design, as DoD plainly intends to make its major suppliers cause all their sources to improve practices to avoid counterfeit electronic parts. Indeed, and DFARS make ''covered contractors'' legally responsible for any counterfeit part that they receive from any supplier, irrespective of size or business orientation, including parts obtained from COTS and commercial sources.

Counterfeit prevention throughout the supply chain, while a commendable objective, creates exposure for ''covered contractors'' because their control over suppliers is limited. Moreover, DFARS implementation will have a cost impact to the extent DoD's large contractors rely upon fewer suppliers who charge higher prices for parts with reduced counterfeit risk. Nowhere is there evidence that DoD has both the intent and the budget to pay these higher costs. DoD's ''covered contractors'' also must anticipate CPSR review of their systems to detect and avoid counterfeit parts. The DFARS lacks guidance on key issues. DCMA has not so far released any official ''guidelines'' for this review, but has pur-

sued a ''checklist'' approach that is being applied differently by each regional DCMA office. Contractors are concerned that DCMA will take a ''strict compliance'' approach that would add to costs and operational disruption and about potential inconsistencies in DCMA methods, measurements and outcomes.

The basic principles of a system to detect and avoid counterfeit parts are straightforward. Contractors are to increase reliance upon ''trusted suppliers'' (original sources and their authorized distributors) and to decrease use of independent distributors and brokers. Where necessary to purchase parts from other than the trusted suppliers, additional measures should be taken to assure authenticity and these measures should reflect the risks associated with the source and potential application of the part. ''Traceability'' is sought to document the history of acquired parts. If found to be ''suspect'' or confirmed as a ''counterfeit,'' a part is to be quarantined and not returned to the supply chain, and appropriate authorities are to be promptly notified. And the rules are to be flowed down to all levels of the supply chain.

The rules apply not only to a diverse set of ''covered contractors'' but, through flowdown, to an even more varied, global supply chain. Contractors need to develop systems that fulfill the purposes of the rule but remain practicable and affordable. Continuity of supply and sustainment must be maintained as these systems are implemented. Similarly, it is important to define ''best practices'' that can serve as benchmarks to assess each company that is subject to the rules. (Even large ''covered contractors'' will find themselves in receipt of flowdown requirements when they are subcontractors.) Recognized best practices should assist ''covered contractors'' in demonstrating to DCMA that their systems are compliant with Section 818 and the DFARS. At lower tiers, ''best practices'' should serve to qualify subcontractors, as having compliant systems, and sources, as being appropriate to use when parts can't be obtained from trusted suppliers. These best practices should reflect existing and emerging industry standards – such as those from SAE, or JEDEC – which are produced through industry-led efforts and are or will be accompanied by independent certification regimes. Industry standards provide a common taxonomy that can be employed by defense and aerospace companies as well as by commercial Information and Communication Technology (ICT) companies. They establish common principles and standard procedures and can be tailored fit company particulars.

The DFARS, at 252.246-7007, sets 12 criteria for a compliant system. Several of these criteria have drawn industry attention as presenting difficult implementation questions. Others depend on still-pending regulations. Six of the criteria are examined below. Industry standards can be very helpful in establishing ''best practices'' which, if accepted by DCMA, would go a long way to showing covered contractors, and their suppliers, how to implement a system that will be found compliant. Other criteria similarly will benefit from recognition and use of industry standards.

(1) Inspection and Testing. For parts other than from trusted suppliers, the DFARS dictates that selection of tests and inspection ''shall be based on minimizing risks to the Government,'' taking into account the ''probability of receiving a counterfeit electronic part,'' whether the chosen methods of inspection and test will detect the counterfeit, and the ''potential negative consequences'' of installation of counterfeit electronic part. Pending SAE AS6171 (''Test Methods Standard: General Requirements, Suspect/Counterfeit Electrical, Electronic and Electromechanical Parts'') will be important as it provides a hierarchy of test methods and a mechanism by which objective risk-based calculations drive selection of appropriate inspection and test methods. AS-6171 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 that recognize how each risk area may be mitigated.

(2) Abolish Proliferation. Responsible contractors know they must avoid the ''return'' of a counterfeit electronic part into the supply chain. Difficulties arise where a contractor deals with brokers/distributors or test labs that have ownership and/or possession of parts found suspect or counterfeit. Various SAE standards address handling of nonconforming product and reporting, e.g., AS6081 (''Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition – Distributors), at 4.2.7 and 4.2.9.

(3) Traceability. The DFARS expects processes to maintain traceability ''back to the original manufacturer'' and dictates that the process shall include documentation developed in accordance with industry standards. It will be very difficult if not impossible to satisfy the literal requirements of this criterion. It applies contemporary (or prospective) practices to parts acquired over many years when such traceability was the norm only for a limited class of MIL SPEC and HI REL parts. This point is recognized, for example, in AS6081 at 4.2.4 (the ''documented process shall require the retention of records providing supply chain traceability *wherever such traceability exists*'') (emphasis added).

(4) Use of Suppliers. A core principle of the DFARS is that the best way to avoid counterfeits is to procure parts from trusted suppliers. However, DoD must support many legacy systems where required parts are obsolete or no longer available from these suppliers. The DFARS is short on guidance on how to qualify additional sources when necessary. Several standards are highly relevant to this crucial function. From the standpoint of the part manufacturer, higher tier purchasing contractors or a maintenance and repair organization, the most relevant standard is AS5553A which provides a complete approach to qualification of suppliers to reduce counterfeit risk. (Rev. B is currently going through an extensive vetting and approval process by relevant industry stakeholders.) Contributing sources include ARP6178, a tool to be used for risk assessment of distributors, and AS6171 (when released), as it describes methods to determine tests and inspections for parts other than those obtained from original sources. SAE AS6081 is focused upon qualification and procedures applicable to brokers and independent distributors and SAE has in development a standard relevant to authorized (franchised) distributors, AS6496.

(5) Reporting & Quarantine. The DFARS criteria require reporting to the Contracting Officer and to the Government Industry Data Exchange Program (GIDEP). The principle that counterfeit and suspect electronic parts should be quarantined is important for

  FCR ISSN 0014-9063

several reasons, most important to prevent re-entry, but also to enable appropriate investigation and law enforcement activity. Reporting is a more complex subject. There are a number of conflicting recommendations pending. The FAR Council, pursuant to FAR Case 2013-002, has issued a proposed rule, ''Expanded Reporting of Nonconforming Items,'' 79 Fed. Reg. 33164 (June 10, 2014) which, when complete, may help clarify or resolve obligations. Several federal agencies and enforcement bodies, such as the National Intellectual Property Rights Coordination Center, have staked out positions seeking to coordinate reporting, but their authority to act as the DFARS requires has not been established. On this issue, the SAE standards do not provide definitive guidance, as the subject of reporting depends upon as yet unresolved regulatory, investigative and law enforcement requirements. AS6081, at 4.2.9, for example, calls for reporting of all occurrences of suspect, fraudulent and confirmed counterfeit parts to ''internal organizations, and to customers, applicable Government authorities, Government reporting organizations (e.g., GIDEP or equivalent), industry reporting programs (e.g., ERAI or equivalent), and Authority Having Jurisdiction.'' This illustrates the many potential recipients of reports but industry will benefit from instructions that are clear and consistent.

(6) Systems to Detect & Avoid. One of the 12 DFARS criteria for system adequacy is the existence of the system itself. The DFARS expressly recognizes that the contractor ''may elect to use current Government- or industry-recognized standards to meet this requirement.'' This may understate the importance of informed reliance upon standards. As noted, about 1,200 contractors are directly subject to the DFARS. They rely upon a supply chain of thousands of vendors, and under the DFARS, the covered contractors must flow down the DFARS and assume some responsibility for the anti-counterfeit compliance of their supply chain. So far as is presently known to the author, DCMA has not completed its first CPSR review of a ''covered contractor's'' system to detect and avoid counterfeit electronic parts. Those reviews should be guided and hopefully expedited by contractor demonstration of adoption, application and adherence to standards that employ risk-based methodologies. Similarly, the ''covered contractors'' cannot individually assess and verify the adherence of each of their vendors, many of whom are not subject to any statutory or regulatory obligation and who therefore will chose the extent to which they will accept DFARS flowdown and how they will implement anti-counterfeiting measures. DCMA and ''covered contractors'' should join to encourage suppliers to adopt counterfeit avoidance measures based upon relevant industry standards. This is good business even if not legally required. As suppliers become certified to the relevant standards, that provides their ''covered contractor'' customers with an objective and verifiable means to demonstrate system adequacy for the supply chain.

The above discussion focuses largely on SAE, because that organization represents a broad technical and operational community and has been very active in the development of standards useful for the aerospace and defense industries. As a generalization, SAE standards are oriented towards purchasers, intermediaries and users of electronic parts. But there is an emerging ''convergence.'' JEDEC, which represents microelectronics manufacturers and suppliers, is working on a proposed standard. It contains many features that align with the DFARS, among them: documented counterfeit mitigation policy; use of authorized distributors and approved suppliers; purchase restrictions favoring trusted suppliers; improved traceability documentation to include Certificate of Conformance; measures to control non-conforming product and to avoid infiltration of counterfeit product into production or inventory; disposition measures that include quarantine and prevention of counterfeits re-entering the supply chain; and others.

It may be tempting for DCMA to develop a DoD-specific plan or DFARS-specific guidelines for anti-counterfeit implementation. Other agencies recently collaborated to produce a ''Strategies Guide'' intended to inform contractors who service NASA and national security space programs on counterfeit prevention. These sector-specific guides can have value, but not if individual contractors are obligated to comply strictly with many similar – but different – requirements. All parties seek cost-effective implementation of anti-counterfeit measures. This argues for flexible and adaptive implementation guidelines, built on risk-based principles, placing principal reliance upon demonstrated adherence to standards-based practices.