Bloomberg BNA

Federal Contracts Report™

Counterfeit Parts

JESD243 is less than what the aerospace and defense industry needs to deal with the threat of counterfeit electronic parts. It serves the interests of semiconductor manufacturers but seems to avoid tough questions. And it offers comparatively little to those in industry or government who face the daily challenge of locating and qualifying parts that are obsolete, no longer in production or unavailable from authorized sources.

BNA INSIGHTS: JEDEC's New JESD243: A New Standard That Is Less Than Industry Needs to Avoid Counterfeit Electronic Parts

By Robert S. Metzger

Increasing attention is being devoted to how standards and best practices can inform and guide industry and provide assurance to public customers as the government seeks to protect itself from supplies and services that are exposed to supply chain threats. Following enactment of Section 818 of the National Defense Authorization Act of FY 2012, the Department of Defense (DOD) issued regulations that require its larger contractors to implement systems to detect and avoid counterfeit electronic parts.

On May 6, 2014, DOD issued a final rule on Detection and Avoidance of Counterfeit Electronic Parts (79 Fed. Reg. 26092). In promulgation comments accompanying the rule, DOD expressed its agreement with use of ''industry consensus standards . . . for the development and implementation of internal counterfeit parts detection and avoidance systems'' (79 Fed. Reg. at 26102). The crux of the 2014 rule is the obligation expressed by DFARS 252.246-7007, that larger contractors must employ counterfeit avoidance systems that satisfy 12 specified criteria. Four of those criteria — inspection and testing (#2), traceability (#4), systems to detect and avoid (#8) and keeping informed (#10) — made explicit reference to industry standards.

Robert Metzger, rmetzger@rjo.com, heads the Washington, D.C., office of Rogers Joseph O'Donnell, PC, a boutique law firm specializing in public contracts. A frequent contributor to Federal Contracts Report, Bob recently was named a ''Federal 100'' awardee by Federal Computer Week for his contributions to cyber and supply chain security. This article reflects Mr. Metzger's personal views and should not be attributed to any client of his firm or organization with which he is involved or affiliated.

More recently, on Sept. 21, 2015, DOD issued a proposed rule that would modify the existing DFARS (80 Fed. Reg. 56939). Even more importance will be assigned to industry standards if these changes are adopted. A DOD contractor will be able to identify ''trustworthy'' suppliers who are other than original sources if the contractor uses ''DoD-adopted counterfeit prevention industry standards'' (see proposed DFARS 246.870-1, 80 Fed. Reg. at 56843). Further, where it is necessary to use a part sourced from a ''non-trusted supplier,'' the proposed DFARS would hold the contractor responsible to inspect, test and authenticate ''in accordance with existing applicable industry standards'' (proposed DFARS 252.246-70XX(d)(2), 80 Fed. Reg. at 56944).[1]

Standards, even after adoption by a sponsoring organization, do not necessarily contribute to solutions to technical problems. A sponsoring organization may not reflect all points of view or consider all aspects of a technical problem.

JEDEC — originally the Joint Electron Devices Engineering Council, now the JEDEC Solid State Technology Association — with nearly 300 members in the microelectronics industry, recently released JESD243, which it claims sets best practices for mitigating counterfeit electronic parts.

JESD243 is less than what the aerospace and defense industry needs to deal with the threat of counterfeit electronic parts. It may have some utility for semiconductor device manufacturers but offers comparatively little to those in industry or government who face the daily challenge of locating and qualifying parts that are obsolete, no longer in production or unavailable from authorized sources.

The message of JESD243 is that the answer to the risk of counterfeit electronic parts is to purchase original parts from the OEM (original equipment manufacturer), or its authorized sales channel, or to pay to have an ''authorized aftermarket manufacturer'' make new batches, with the OEM's authorization, of an otherwise unavailable part.

This focus does not address the continuing demand for parts not now available from OEMs. It also neglects the millions of electronic parts that may be authentic and satisfy customer requirements but which now have left the OEM's controlled distribution channels. From the standpoint of the sustainment community, an industry standard that insists upon purchase of parts exclusively from OEMs or aftermarket manufacturers is neither realistic nor responsive.

JEDEC and the Purposes of JESD243

JEDEC, according to its website, is ''the global leader in developing open standards for the microelectronics industry.'' On March 24, it announced the publication of JESD243: *Counterfeit Electronic Parts: Non-Proliferation for Manufacturers*.

According to the organization's press release, this standard identifies the best commercial practices for mitigating and/or avoiding counterfeit products. JESD243, directed at ''all manufacturers of electronic parts,'' is described as defining ''standard requirements for developing both a mitigation policy and a product return policy, including return verification and a prohibition on the restocking of confirmed counterfeit parts.''[2]

JESD243 is promoted as helping manufacturers ''stem the tide of counterfeit electronic parts.'' It may be useful to device manufacturers, in a self-serving sense, because it accommodates existing and individual business practices that maximize the market opportunity of manufacturers. It has less utility to those who build and support systems that use electronic devices. The most acute threat from counterfeit electronics often arises in sustainment of systems where the needed part is no longer in production or available from original (or ''trusted'') sources. JESD243 does not address this chronic and continuing problem. It contemplates purchase only from the original device maker, its authorized distributors, or approved aftermarket manufacturers. This is not an affordable or timely answer where companies seek to sustain equipment for which parts *are no longer available from those trusted sources*.

One objective of an industry standard, presumably, is to inform both those who produce and those who buy that a resource conforms to that standard. JESD243 lacks substance. It calls upon device manufacturers to adopt policies and plans but provides little detail as to what measures are to be employed as ''best practices.'' The value of JESD243 is diluted by the absence of defining details. Its vagueness serves to protect typical practices of device manufacturers rather than improve them. In contrast to other industry standards, such as AS553A or others put out by SAE International, JESD243 does not express and elaborate upon norms, best practices or technical methods.

Critique of Key Features

JESD243 begins (in ''Scope,'' in item 1) with a statement that it ''identifies the best commercial practices for mitigating and/or avoiding counterfeit products by all manufacturers of electronic parts.'' This may promise more than JESD243 delivers. Under ''Requirements,'' it calls for a counterfeit mitigation policy which must be documented, but it provides no substantive particulars needed to know what is satisfactory. Largely, it is a ''policy of policies,'' calling not for specific or consistent measures but for individual manufacturers to make their own choices in how to implement these policies.

Over time, a number of areas of technical and business practice have emerged as focus areas for efforts to detect and avoid counterfeit parts. Too often, the content of JESD243 on these subjects is insubstantial.

Reporting: The master policy (at 4.1) calls for policies for disposition and reporting of parts determined to be

[1] For further discussion of the value of standards to the fight against counterfeits, see my previous article, *View From RJO: A Standards-Based Way to Avoid Counterfeit Electronic Parts*, 102 FCR 540, Nov. 4, 2014. In that article, I wrote about an ''emerging 'convergence' '' with the standard then being worked on by JEDEC. I observed that it contained many features that align with the counterfeit parts DFARS. Unfortunately, as explained in this article, the final JEDEC standard, JESD243, identifies relevant subjects but rarely goes beyond the surface of the issue. As industry experience has evolved, JESD243 seems ''thin'' by comparison with the work of other standards-setting bodies.

[2] Press Release, JEDEC, New JEDEC Standard Sets Best Practices for Mitigating Counterfeit Electronic Parts (Mar. 24, 2016).

  FCR ISSN 0014-9063

counterfeit. But JESD243 states no obligation or even preference on which party in the supply chain (e.g., supplier, customer, independent third party, or certified laboratory) is to report a counterfeit. While JESD243 recognizes the existence of GIDEP (the Government Industry Data Exchange Program), it is up to the manufacturer (by 4.3.3 d)) to determine whether it considers it ''appropriate'' to notify GIDEP. JESD243 ignores altogether valuable commercial sources of information on product nonconformity, such as ERAI (*www.erai.com*) and makes no reference to any other reporting instrumentalities or obligations.

Plan Requirements: Manufacturers are called upon (at 4.2) to develop and implement a ''counterfeit parts control plan'' but the ''minimum processes'' called out as requirements are largely protective of OEMs as exclusive sources of supply. Few details are provided, beyond an assembly of high-level requirements such as, for example, maintenance of lists of authorized distributors and approved suppliers, use of an approved distribution agreement, restrictions on sources for purchases of parts and raw materials, and suggestions as to delivery documentation.

Authorized Distributors: While JESD243 strongly favors use of authorized distributors, the standard contains virtually no minimum requirements for selecting and maintaining such distributors. The JESD treatment is modest by comparison to the approach of SAE AS6081 (''Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition – Distributors''), which goes into great length to discuss appropriate handling, material and inventory control, quality processes, and detection criteria for counterfeit parts, traceability, and the like.

Minimum Processes: The ''minimum processes'' (at 4.2.1 – 4.2.9) are stated only generally and may serve more to justify existing practices rather than improve measures that device manufacturers employ to control their supply chain. This approach may be helpful to the ''supply'' side of the supply chain but is less so to the ''demand'' side because it offers little granularity to assure device purchasers.

JESD243 considers the objectives of the device manufacturer but not the needs of those who support as well as build equipment that use electronic parts. Little benefit is rendered to other supply chain participants (non-franchised distributors, hardware operators, maintenance and support contractors) who regularly confront risk of counterfeit electronic parts where original sources are exhausted.

Supply Chain Traceability: JESD243 includes (at item 3) an elaborate definition of ''supply chain traceability'' – but there is no general obligation imposed upon device manufacturers to ensure that their products, once delivered, are traceable either through accompanying documentation or through technical means to verify authenticity.

The only reference to traceability in the operative portions of JESD243 is under the heading of ''return verification'' (at 4.3.2); before a manufacturer restocks parts returned to it, it must validate the parts against the traceability records. This serves the interest of the manufacturer — but not the needs of the system purchaser, operator or maintenance provider. This falls short of meeting the ''provenance'' objective that many supply chain professionals seek to assure that electronic parts are authentic and have not been exposed to substitution or tampering.

'Permissive' Requirements: JESD243 is ''permissive'' in sensitive but important areas. Consider 4.3.3 (''Disposition of returns deemed suspect or counterfeit''), for example. Even as to parts confirmed as counterfeit, JESD243 contains no absolute or unqualified instruction to the entity ''on the spot'' (which could be a supplier, customer, independent third party or certified laboratory, etc.) as to disposition, whether it be to quarantine or destroy. The document advises that confirmed counterfeits shall not be returned to the customer, but the manufacturer ''may'' (and hence, ''may not'') decide to retain them or to turn over to law enforcement.

No obligation is present either to preserve evidence for law enforcement or to inform potentially at-risk users who may already have received or installed a known counterfeit. Nor is any ''best practice'' stated for forensic investigation to determine the source of the counterfeit or to take measures to act against such sources.

Return Verification: If parts are returned to the manufacturing organization, the manufacturing organization (by 4.3.2) is obliged to perform ''return verification'' before return of parts to stock or resale. Left unspecified is how and with what methods or test to perform the ''return verification.'' Therefore, these important questions — exactly in the domain where technical standards often operate — are left entirely to the discretion of each manufacturer.

Certificates of Conformance: A certificate of conformance (CoC) is an important legal and contractual instrument to assure buyers of authenticity and to document the manufacturer's commitment. JESD243 (at 4.2.7) leaves it to each manufacturer's ''internal procedures'' to determine whether and with what content a CoC will be provided.

Had it established minimum and sufficient CoC obligations, JEDEC could better serve the interests of buyers and other downstream supply chain participants. JESD243 states that CoC ''data content *may include*'' (emphasis added) enumerated subjects, such as the name of the manufacturing organization, the part number, date and lot code, etc. There is no reason — either stated or apparent — to leave the details of CoC data content entirely to the discretion of each manufacturer and not to specify at least CoC ''minimums,'' and identify other useful but elective content. Buyers and downstream recipients of electronic parts rely on the CoC for ''provenance'' assurance.

Production Overruns: JESD243 does not obligate manufacturers to strictly control production overruns. A ''policy'' and ''methodology'' are required (by 4.2.9) to keep these from re-entering the supply chain, but no particulars are provided (as to how, when, what, using which standards, and so forth), and therefore JESD243 again falls short of what an industry standard could do to establish a reliable process to avoid improper distribution of such parts.

Verifying Authenticity: Technical methods are available to determine the authenticity of electronic parts. JESD243 provides little content on this important subject, even though many technical means are employed by manufacturers and test specialists, and others are emerging. (SAE is in the final stages of completing SAE AS6171, ''Test Methods Standard; General Requirements, Suspect/Counterfeit, Electrical, Electronic, and Electromechanical Parts.'')

Surprisingly, JESD243 does not consider the present utilization by semiconductor makers of sophisticated (often proprietary) methods to uniquely identify their products. Nor does it facilitate the ability of customers and users to verify authenticity by reference to such methods and unique device signatures.

Life Cycle Issues: Life cycle issues for electronic components are closely related to exposure to counterfeit electronic parts. When parts enter obsolescence, are out of production, or when there are diminishing manufacturing sources and material shortages (DMSMS), there is greater risk of counterfeits. In the defense sector, the issue is especially acute. The production life cycle for discrete commercial electronic parts often is measured in a few years while those parts may be used in defense systems (or in critical infrastructure) for decades.

Yet, the concepts of ''product life cycle,'' ''components obsolescence'' and ''diminishing sources'' are *entirely absent* from JESD243. No responsibility is assigned to device manufacturers to plan for these conditions or to inform customers and operators when these conditions are imminent. Nor is there any duty of cooperation to address technical solutions (emulation, cooperation to facilitate contract manufacture, etc.) to parts shortages. It is a great disappointment that JEDEC did not address these known problems and pressing subjects.

Aftermarket Manufacturers: JESD243 is written primarily for the benefit of original manufacturers. Considering the source, and its purpose, its restrictive approach to qualification of substitute manufacturers is unsurprising. However, in the definition of ''authorized aftermarket manufacturer,'' JESD243 excludes entirely the possibility that an obsolete or unavailable device can be ''reverse-engineered'' successfully — *and legally* — without the permission of the rights holder of the original intellectual property (IP).

JESD243 limits reverse-engineering to situations where there is no violation of the IP rights of the original manufacturer *and* where ''*authorization*'' has been obtained from the original manufacturer or IP rights holder. Moreover, JESD243 is not entirely clear whether an ''authorized aftermarket manufacturer'' must inform customers that a part it has produced (with the IP holder's authorization) is different from the original.

The definition requires the part to ''match'' all the specifications of the original component manufacturer ''and satisfy customer needs'' but that leaves room for different internal configuration which may not be disclosed to the customer. JESD243 does not establish either qualification standards or verification measures for ''authorized aftermarket manufacturers.''

Records Retention: The ''retention of records'' feature (at 4.2.8) appears cursory and deferential to company election rather than prescriptive of ''best practices'' or expected, ''standard'' methods. It says that a manufacturing organization shall ''document and maintain records in accordance with their internal quality system standards.''

Records are to be suitable in ''format, accuracy, and detail to permit analysis by the *organizations* internal quality personnel and government agencies.'' (Emphasis in original.) When questions arise about parts authenticity, OEMs could help if they retain information on design/build and other technical data and agree to make that information available when needed by customers, government agencies and others in the supply chain to validate parts authenticity. JESD243 does not recognize the interests of customers in the content or availability of retained records.

Conclusion

Holistically, JESD243 seeks to protect the ability of device manufacturers to assure customers of authenticity when they purchase electronic parts exclusively from the original maker, its authorized distributors or approved aftermarket manufacturers. JESD243 does not address how customers and operators of electronic systems are to address risks of counterfeits that arise when needed electronic parts cannot be obtained from the trusted sources.

JESD243 provides little analysis and few prescriptions of how manufacturers can help to identify, address and respond to counterfeit threats when buyers must go outside trusted sources for parts. It is notably devoid of technical content even though sophisticated manufacturers of electronic devices are the ostensible audience.

Defense contractors — especially but not exclusively — have long-term sustainment obligations. Purchasers in this context would benefit greatly from cooperation of the OEM to document ''provenance'' and to establish authenticity where in question. In this sense, JEDEC's approach does not reflect or respond to market conditions. JEDEC does not help purchasers of parts from non-franchised distributors reduce risks through informed test and inspection. In the real world, non-franchised distributors may be the only sources for some necessary parts. Other organizations, such as SAE and the Defense Logistics Agency, have taken effective measures to improve buyer assurance when they use a distributor.

JEDEC could have done more to help aerospace and defense industries. It could have made positive and specific commitments to reporting of counterfeit parts, taken a stronger position on quarantine, imposed specific standards for traceability, and done more to establish the details of manufacturer methods to avoid counterfeits in their distribution chain. JEDEC also could have accepted a responsibility to offer information and technical support for third-party risk mitigation measures, such as additional test and inspection. Perhaps in later versions, these features will be added, and JESD243 will contribute more to industrywide efforts to detect and avoid counterfeit electronic parts.

Standards-setting organizations might be informed by this commentary. In many areas of cyber and supply chain security, participants at all levels of the supply chain are looking for standards and best practices to guide and instruct, and to give confidence to buyers and users. While standards should not be proscriptive where flexibility is needed, they should contain sufficient method and detail to add to industry's response to known and evolving risks.

  FCR ISSN 0014-9063